NetApp® CN1610 Network Switch
CLI Command Reference

NetApp, Inc.
495 East Java Drive
Sunnyvale, CA 94089 U.S.A.
Telephone: +1 (408) 822-6000
Fax: +1 (408) 822-4501
Support telephone: +1 (888) 463-8277
Documentation comments: doccomments@netapp.com
Information Web: www.netapp.com

Part number: 215-06286_C0
August 2017

Copyright and trademark information

Copyright information

Trademark information

Table of Contents

About This Document 1

Introduction

This document describes command-line interface (CLI) commands you use to view and configure the CN1610 software. You can access the CLI by using a direct connection to the serial port or by using Telnet or SSH over a remote network connection.

Note

Some commands in this document may not be available with your version of the FASTPATH software. Enter a question mark (?) after typing one or more characters of a word to list the available commands or parameters that begin with the letters. See "Using CLI Help" on page 25 for more information.

Audience

This document is for system administrators who configure and operate systems using FASTPATH® software. It provides an understanding of the configuration options of the FASTPATH software.

Software engineers who integrate FASTPATH software into their hardware platform can also benefit from a description of the configuration options.

This document assumes that you have an understanding of the FASTPATH software base and have read the appropriate specification for the relevant networking device platform. It also assumes that you have a basic knowledge of Ethernet and networking concepts.

Refer to the release notes for the FASTPATH application-level code. The release notes detail the platform-specific functionality of the Switching, SNMP, Configuration, Management, and other packages. The suite of features the FASTPATH packages support is not available on all the platforms to which FASTPATH software has been ported.

About FASTPATH Software

FASTPATH software has two purposes:

- Assist attached hardware in switching frames, based on Layer 2, 3, or 4 information contained in the frames.
- Provide a complete device management portfolio to the network administrator.

Scope

FASTPATH software encompasses both hardware and software support. The software is partitioned to run in the following processors:

- CPU

  This code runs the networking device management portfolio and controls the overall networking device hardware. It also assists in frame forwarding, as needed and specified. This code is designed to run on multiple platforms with minimal changes from platform to platform.

- Networking device processor

  This code does the majority of the packet switching, usually at wire speed. This code is platform-dependent, and substantial changes might exist across products.

Product Concept

Fast Ethernet and Gigabit Ethernet switching continues to evolve from high-end backbone applications to desktop switching applications. The price of the technology continues to decline, while performance and feature sets continue to improve. Devices that are capable of switching Layers 2, 3, and 4 are increasingly in demand. FASTPATH software provides a flexible solution to these ever-increasing needs.

The exact functionality provided by each networking device on which the FASTPATH software base runs varies depending upon the platform and requirements of the FASTPATH software.

FASTPATH software includes a set of comprehensive management functions for managing both FASTPATH software and the network. You can manage the FASTPATH software by using one of the following two methods:

- Command-Line Interface (CLI)
- Simple Network Management Protocol (SNMP)

Each of the FASTPATH management methods enables you to configure, manage, and control the software locally or remotely using in-band or out-of-band mechanisms. Management is standards-based, with configuration parameters and a private Management Information Base (MIB) providing control for functions not completely specified in the MIBs.

Using the Command-Line Interface 2

About this chapter

The command-line interface (CLI) is a text-based way to manage and monitor the system. You can access the CLI by using a direct serial connection or by using a remote logical connection with Telnet or SSH.

Topics in this chapter

This chapter describes the CLI syntax, conventions, and modes. It contains the following sections:

Command Syntax

A command is one or more words that might be followed by one or more parameters. Parameters can be required or optional values.

Some commands, such as `show network` or `clear vlan`, do not require parameters. Other commands, such as `network parms`, require that you supply a value after the command. You must type the parameter values in a specific order, and optional parameters follow required parameters. The following example describes the `network parms` command syntax:
`network parms ipaddr netmask [gateway]`

- `network parms` is the command name.
- `ipaddr` and `netmask` are parameters and represent required values that you must enter after you type the command keywords.
- `[gateway]` is an optional parameter, so you are not required to enter a value in place of the parameter.

The *NetApp CN1610 Network Switch CLI Command Reference* lists each command by the command name and provides a brief description of the command. Each command reference also contains the following information:

- Format shows the command keywords and the required and optional parameters.
- Mode identifies the command mode you must be in to access the command.
- Default shows the default value, if any, of a configurable setting on the device.

The `show` commands also contain a description of the information that the command shows.

Command Conventions

The parameters for a command might include mandatory values, optional values, or keyword choices. Parameters are order-dependent. The following Parameter Conventions table describes the conventions this document uses to distinguish between value types:

Symbol	Example	Description
[] square brackets	`[value]`	Indicates an optional parameter.
italic font in a parameter.	*value* or [*value*]	Indicates a variable value. You must replace the italicized text and brackets with an appropriate value, which might be a name or number.
{ } curly braces	{choice1 | choice2}	Indicates that you must select a parameter from the list of choices.
| Vertical bars	choice1 | choice2	Separates the mutually exclusive choices.
[{ }] Braces within square brackets	[{choice1|choice2}]	Indicates a choice within an optional element.

Common Parameter Values

Parameter values might be names (strings) or numbers. To use spaces as part of a name parameter, enclose the name value in double quotes. For example, the expression “System Name with Spaces” forces the system to accept the spaces. Empty strings (““) are not valid user-defined strings. The following Parameter Descriptions table describes common parameter values and value formatting:

Parameter	Description

ipaddr	This parameter is a valid IP address. You can enter the IP address in the following formats:
	`a (32 bits)`
	`a.b (8.24 bits)`
	`a.b.c (8.8.16 bits)`
	`a.b.c.d (8.8.8.8)`
	In addition to these formats, the CLI accepts decimal, hexadecimal, and octal formats through the following input formats (where *n* is any valid hexadecimal, octal or decimal number):
	`0xn` (CLI assumes hexadecimal format.)
	`0n` (CLI assumes octal format with leading zeros.)
	`n` (CLI assumes decimal format.)

ipv6-address	`FE80:0000:0000:0000:020F:24FF:FEBF:DBCB,` or
	`FE80:0:0:0:20F:24FF:FEBF:DBCB, or`
	`FE80::20F24FF:FEBF:DBCB, or`
	`FE80:0:0:0:20F:24FF:128:141:49:32`
	For additional information, refer to RFC 3513.

Interface or slot/port	Valid slot and port number separated by a forward slash. For example, 0/1 represents slot number 0 and port number 1.
Logical Interface	Represents a logical slot and port number. This is applicable in the case of a port-channel (LAG). You can use the logical slot/port to configure the port-channel.

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

Interface Naming Convention

FASTPATH software references physical entities such as cards and ports by using a slot/port naming convention. The FASTPATH software also uses this convention to identify certain logical entities, such as link aggregation groups (LAGs), which are also known as port-channels.

When a command indicates that the variable is *slot/port*, an example of a valid entry is 0/1. This represents slot 0, port 1 on the switch. To configure port 12, the slot/port to enter would be 0/12.

To configure a LAG, which is a group of ports acting as a single interface, you enter the keyword `lag` followed by the LAG number, for example `lag 2`.

For many commands, you can also specify a range of physical or LAG interfaces to configure at the same time with the same settings. To specify a range of interfaces, the slot/port is separated by a dash, for example 0/1-0/4 indicates that the same settings will apply to ports 1, 2, 3, and 4.

The slot number has two uses. In the case of physical ports, it identifies the card containing the ports. In the case of logical and CPU ports it also identifies the type of interface or port.

Slot Type	Description
Physical slot numbers	Physical slot numbers begin with zero, and are allocated up to the maximum number of physical slots.
CPU slot numbers	The CPU slots immediately follow the logical slots.

The port identifies the specific physical port being managed on a given slot.

Port Type	Description
Physical ports	The physical ports for each slot are numbered sequentially starting from zero.
CPU ports	CPU ports are handled by the driver as one or more physical entities located on physical slots.

Using the no Form of a Command

The `no` keyword is a specific form of an existing command and does not represent a new or distinct command. Almost every configuration command has a `no` form. In general, use the `no` form to reverse the action of a command or reset a value back to the default. For example, the `no shutdown` configuration command reverses the shutdown of an interface. Use the command without the keyword `no` to re-enable a disabled feature or to enable a feature that is disabled by default. Only the configuration commands are available in the `no` form.

CN1610 Software Modules

The CN1610 software consists of flexible modules that can be applied in various combinations to develop advanced Layer 2/3/4+ products. The commands and command modes available on your switch depend on the installed modules. Additionally, for some `show` commands, the output fields might change based on the modules included in the CN1610 software.

The CN1610 software suite includes the following modules:

- Switching (Layer 2)
- Quality of Service
- Management (CLI and SNMP)
- IPv6 Management—Allows management of the CN1610 switch through an IPv6 address without requiring any IPv6 Routing features in the system. The management address can be associated with the network port (front-panel switch ports), a routine interface (port or VLAN), and the Service port.
- Security

Command Modes

The CLI groups commands into modes according to the command function. Each of the command modes supports specific CN1610 software commands. The commands in one mode are not available until you switch to that particular mode, with the exception of the User EXEC mode commands. You can execute the User EXEC mode commands in the Privileged EXEC mode.

The command changes in each command mode to help you identify the current mode. The following CLI Command Modes table describes the command modes and the prompts visible in that mode:

Command Mode	Prompt	Mode Description
User EXEC	`(CN1610)>`	Contains a limited set of commands to view basic system information.
Privileged EXEC	`(CN1610)#`	Allows you to enter any `EXEC` command, enter the VLAN mode, or enter the Global Configuration mode.
Global Config	`(CN1610) (Config)#`	Groups general setup commands and permits you to make modifications to the running configuration.
VLAN Config	`(CN1610)(Vlan)#`	Groups all the VLAN commands.

Command Mode	Prompt	Mode Description

Interface Config	`(CN1610) (Interface slot/port)#`
	
	`(CN1610) (Interface slot/port (startrange)-slot/port(endrange) #`
		Manages the operation of an interface.
		Use this mode to set up a physical port for a specific logical connection operation.
		You can also use this mode to manage the operation of a range of interfaces. For example, the prompt may display as follows: `(CN1610) (Interface 0/1-0/4) #`

Line Console	`(CN1610) (config-line)#`	Contains commands to configure outbound Telnet settings and console interface settings, as well as to configure console login/enable authentication.
Line SSH	`(CN1610) (config-ssh)#`	Contains commands to configure SSH login/enable authentication.
Line Telnet	`(CN1610) (config-telnet)#`	Contains commands to configure Telnet login/enable authentication.
AAA IAS User Config	`(CN1610) (Config-IAS-User)#`	Allows password configuration for a user in the IAS database.

Command Mode	Prompt	Mode Description
Mail Server Config	`(CN1610) (Mail-Server)#`	Allows configuration of the email server.
Policy Map Config	`(CN1610) (Config-policy-map)#`	Contains the QoS Policy-Map configuration commands.
Policy Class Config	`(CN1610) (Config-policy-class-map)#`	Consists of class creation, deletion, and matching commands. The class match commands specify Layer 2, Layer 3, and general match criteria.
Class Map Config	`(CN1610) (Config-class-map)#`	Contains the QoS class map configuration commands for IPv4.
MAC Access-list Config	`(CN1610) (Config-mac-access-list)#`	Allows you to create a MAC Access-List and to enter the mode containing MAC Access-List configuration commands.
TACACS Config	`(CN1610) (Tacacs)#`	Contains commands to configure properties for the TACACS servers.
ARP Access-List Config Mode	`(CN1610) (Config-arp-access-list)#`	Contains commands to add ARP ACL rules in an ARP Access List.

The following CLI Mode Access and Exit table explains how to enter or exit each mode:

Command Mode	Prompt	Mode Description
User EXEC	This is the first level of access.	To exit, enter `logout`.
Privileged EXEC	From the User EXEC mode, enter `enable`.	To exit to the User EXEC mode, enter `exit` or press `Ctrl-Z`.
Global Config	From the Privileged EXEC mode, enter `configure`.	To exit to the Privileged EXEC mode, enter `exit`, or press `Ctrl-Z`.
VLAN Config	From the Privileged EXEC mode, enter `vlan database`.	To exit to the Privileged EXEC mode, enter `exit`, or press `Ctrl-Z`.
Interface Config	From the Global Config mode, enter: `interface slot/port` or `interface slot/port(startrange)-slot/port(endrange)`	To exit to the Global Config mode, enter `exit`. To return to the Privileged EXEC mode, enter `Ctrl-Z`.
Line Console	From the Global Config mode, enter `line console`.	To exit to the Global Config mode, enter `exit`. To return to the Privileged EXEC mode, enter `Ctrl-Z`.
AAA IAS User Config	From the Global Config mode, enter `aaa ias-user username name`.	To exit to the Global Config mode, enter `exit`. To return to the Privileged EXEC mode, enter `Ctrl-Z`.

Command Mode	Prompt	Mode Description
Mail Server Config	From the Global Config mode, enter `mail-server address.`	To exit to the Global Config mode, enter `exit`. To return to the Privileged EXEC mode, enter `Ctrl-Z`.
Policy-Map Config	From the Global Config mode, enter `policy-map`.	To exit to the Global Config mode, enter `exit`. To return to the Privileged EXEC mode, enter `Ctrl-Z`.
Policy-Class-Map Config	From the Policy Map mode, enter `class`.	To exit to the Policy Map mode, enter `exit`. To return to the Privileged EXEC mode, enter `Ctrl-Z`.
Class-Map Config	From the Global Config mode, enter `class-map`, and specify the optional keyword `ipv4` to specify the Layer 3 protocol for this class.	To exit to the Global Config mode, enter `exit`. To return to the Privileged EXEC mode, enter `Ctrl-Z`.
MAC Access-list Config	From the Global Config mode, enter `mac access-list extended name`.	To exit to the Global Config mode, enter `exit`. To return to the Privileged EXEC mode, enter `Ctrl-Z`.
TACACS Config	From the Global Config mode, enter `tacacs-server host ip-addr`, where `ip-addr` is the IP address of the TACACS server on your network.	To exit to the Global Config mode, enter `exit`. To return to the Privileged EXEC mode, enter `Ctrl-Z`.

Command Mode	Prompt	Mode Description
ARP Access-List Config Mode	From the Global Config mode, enter the `arp access-list command`.	To exit to the Global Config mode, enter the `exit` command. To return to the Privileged EXEC mode, enter `Ctrl-Z`.

Command Completion and Abbreviation

Command completion finishes spelling the command when you type enough letters of a command to uniquely identify the command keyword. Once you have entered enough letters, press the SPACEBAR or TAB key to complete the word.

Command abbreviation allows you to execute a command when you have entered enough letters to uniquely identify the command. You must enter all of the required keywords and parameters before you enter the command.

CLI Error Messages

If you enter a command and the system is unable to execute it, an error message appears. The following table describes the most common CLI error messages:

Message Text	Description
% Invalid input detected at '^' marker.	Indicates that you entered an incorrect or unavailable command. The carat (^) shows where the invalid text is detected. This message also appears if any of the parameters or values are not recognized.
Command not found / Incomplete command. Use ? to list commands.	Indicates that you did not enter the required keywords or values.
Ambiguous command	Indicates that you did not enter enough letters to uniquely identify the command.

CLI Line-Editing Conventions

The following CLI editing conventions table describes the key combinations you can use to edit commands or increase the speed of command entry. You can access this list from the CLI by entering `help` from the User or Privileged EXEC modes.

Key Sequence	Description
DEL or Backspace	Delete previous character.
Ctrl-A	Go to beginning of line.
Ctrl-E	Go to end of line.
Ctrl-F	Go forward one character.
Ctrl-B	Go backward one character.
Ctrl-D	Delete current character.
Ctrl-U, X	Delete to beginning of line.
Ctrl-K	Delete to end of line.
Ctrl-W	Delete previous word.
Ctrl-T	Transpose previous character.
Ctrl-P	Go to previous line in history buffer.
Ctrl-R	Rewrites or pastes the line.
Ctrl-N	Go to next line in history buffer.
Ctrl-Y	Prints last deleted character.
Ctrl-Q	Enables serial flow.
Ctrl-S	Disables serial flow.
Ctrl-Z	Return to root command prompt.
Tab, <SPACE>	Command-line completion.
Exit	Go to next lower command prompt.

Key Sequence	Description
?	List available commands, keywords, or parameters.

Using CLI Help

Enter a question mark (?) at the command prompt to display the commands available in the current mode:

```
(CN1610)>?


enable      Enter into user privilege mode.
help        Display help for various special keys.
logout      Exit this session. Any unsaved changes are lost.
password    Change an existing user's password.
ping        Send ICMP echo packets to a specified IP address.
quit        Exit this session. Any unsaved changes are lost.
show        Display Switch Options and Settings.
telnet      Telnet to a remote host.
```

Enter a question mark (?) after each word you enter to display available command keywords or parameters:

```
(CN1610)#network ?


ipv6          Configure IPv6 parameters for system network.
mac-address   Configure MAC Address.
mac-type      Select the locally administered or burnedin MAC
              address.
mgmt_vlan     Configure the Management VLAN ID of the switch.
parms         Configure Network Parameters of the device.
protocol      Select DHCP, BootP, or None as the network config
              protocol.
```

If the help output shows a parameter in angle brackets, you must replace the parameter with a value:

```
(CN1610)#network parms ?
<ipaddr>    Enter the IP address.
```

If there are no additional command keywords or parameters, or if additional parameters are optional, the following message appears in the output:

```
<cr>        Press Enter to execute the command
```

You can also enter a question mark (?) after typing one or more characters of a word to list the available command or parameters that begin with the letters, as shown in the following example:

```
(CN1610) #show m?

mac                     mac-addr-table          mac-address-table
mail-server             mbuf                    mldsnooping
monitor                 msg-queue
```

Accessing the CLI

You can access the CLI by using a direct console connection or by using a Telnet or SSH connection from a remote management host.

For the initial connection, you must use a direct connection to the console port. You cannot access the system remotely until the system has an IP address, subnet mask, and default gateway. You can set the network configuration information manually, or you can configure the system to accept these settings from a BOOTP server on your network. For more information, see “Console Port Access Commands” on page 38.

Management Commands 3

This chapter describes the management commands available in the FASTPATH CLI.

The Management Commands chapter contains the following sections:

The commands in this chapter are in one of three functional groups:

- Show commands display switch settings, statistics, and other information.
- Configuration commands configure features and options of the switch. For every configuration command, there is a `show` command that displays the configuration setting.
- Clear commands clear some or all of the settings to factory defaults.

Network Interface Commands

This section describes the commands you use to configure a logical interface for management access. To configure the management VLAN, see “network mgmt_vlan” on page 351.

enable (Privileged EXEC access)

This command gives you access to the Privileged EXEC mode. From the Privileged EXEC mode, you can configure the network interface.

Format	`enable`
Mode	User EXEC

do (Privileged EXEC commands)

This command executes Privileged EXEC mode commands from any of the configuration modes.

Format	`do` *`Priv Exec Mode Command`*
Mode	◆ Global Config ◆ Interface Config ◆ VLAN Config

The following is an example of the *`do`* command that executes the Privileged EXEC command *`script list`* in Global Config Mode.

```
(CN1610) #configure

(CN1610)(config)#do script list

Configuration Script Name        Size(Bytes)
-------------------------------- -----------
backup-config                           2105
running-config                          4483
startup-config                           445

3 configuration script(s) found.
2041 Kbytes free.
```

serviceport ip

This command sets the IP address, the netmask and the gateway of the network management port. You can specify the *none* option to clear the IPv4 address and mask and the default gateway (i.e., reset each of these values to 0.0.0.0).

Format	`serviceport ip {`*`ipaddr netmask`* `[`*`gateway`*`] | none}`
Mode	Privileged EXEC

serviceport protocol

This command specifies the network management port configuration protocol. If you modify this value, the change is effective immediately. If you use the *bootp* parameter, the switch periodically sends requests to a BootP server until a response is received. If you use the *dhcp* parameter, the switch periodically sends requests to a DHCP server until a response is received. If you use the *none* parameter, you must configure the network information for the switch manually.

Format	`serviceport protocol {none | bootp | dhcp}`
Mode	Privileged EXEC

serviceport protocol dhcp

This command enables the DHCPv4 client on a Service port.

Default	none
Format	`serviceport protocol dhcp`
Mode	Privileged EXEC

The following shows an example of the command.

```
(CN1610) # serviceport protocol dhcp
```

network parms

This command sets the IP address, subnet mask and gateway of the device. The IP address and the gateway must be on the same subnet. When you specify the *none* option, the IP address and subnet mask are set to the factory defaults.

Format	`network parms {`*`ipaddr netmask`* `[`*`gateway`*`]| none}`
Mode	Privileged EXEC

network protocol

This command specifies the network configuration protocol to be used. If you modify this value, change is effective immediately. If you use the *bootp* parameter, the switch periodically sends requests to a BootP server until a response is received. If you use the *dhcp* parameter, the switch periodically sends requests to a DHCP server until a response is received. If you use the *none* parameter, you must configure the network information for the switch manually.

Default	none
Format	`network protocol {none | bootp | dhcp}`
Mode	Privileged EXEC

network protocol dhcp

This command enables the DHCPv4 client on a Network port.

Default	none
Format	`network protocol dhcp`
Mode	Global Config

The following shows an example of the command.

```
(CN1610) # network protocol dhcp
```

network mac-address

This command sets locally administered MAC addresses. The following rules apply:

- Bit 6 of byte 0 (called the U/L bit) indicates whether the address is universally administered (b'0') or locally administered (b'1').
- Bit 7 of byte 0 (called the I/G bit) indicates whether the destination address is an individual address (b'0') or a group address (b'1').
- The second character, of the twelve character macaddr, must be 2, 6, A or E.

A locally administered address must have bit 6 On (b'1') and bit 7 Off (b'0').

Format	`network mac-address` *`macaddr`*
Mode	Privileged EXEC

network mac-type

This command specifies whether the switch uses the burned in MAC address or the locally-administered MAC address.

Default	burnedin
Format	`network mac-type {local | burnedin}`
Mode	Privileged EXEC

no network mac-type

This command resets the value of MAC address to its default.

Format	`no network mac-type`
Mode	Privileged EXEC

show network

This command displays configuration settings associated with the switch's network interface. The network interface is the logical interface used for in-band connectivity with the switch via any of the switch's front panel ports. The configuration parameters associated with the switch's network interface do not affect the configuration of the front panel ports through which traffic is switched or routed. The network interface is always considered to be up, whether or not any member ports are up; therefore, the `show network` command will always show Interface Status as Up.

Format	`show network`
Modes	◆ Privileged EXEC ◆ User EXEC

Term	Definition
Interface Status	The network interface status; it is always considered to be “up”.
IP Address	The IP address of the interface. The factory default value is 0.0.0.0.
Subnet Mask	The IP subnet mask for this interface. The factory default value is 0.0.0.0.

Term	Definition
Default Gateway	The default gateway for this IP interface. The factory default value is 0.0.0.0.
IPv6 Administrative Mode	Whether enabled or disabled.
IPv6 Prefix is	The IPv6 address and length. Default is Link Local format.
Burned In MAC Address	The burned in MAC address used for in-band connectivity.
Locally Administered MAC Address	If desired, a locally administered MAC address can be configured for in-band connectivity. To take effect, 'MAC Address Type' must be set to 'Locally Administered'. Enter the address as twelve hexadecimal digits (6 bytes) with a colon between each byte. Bit 1 of byte 0 must be set to a 1 and bit 0 to a 0, i.e. byte 0 should have the following mask 'xxxx xx10'. The MAC address used by this bridge when it must be referred to in a unique fashion. It is recommended that this be the numerically smallest MAC address of all ports that belong to this bridge. However it is only required to be unique. When concatenated with dot1dStpPriority a unique Bridge Identifier is formed which is used in the Spanning Tree Protocol.
MAC Address Type	The MAC address which should be used for in-band connectivity. The choices are the burned in or the Locally Administered address. The factory default is to use the burned in MAC address.
Configured IPv4 Protocol	The IPv4 network protocol being used. The options are bootp | dhcp | none.
Configured IPv6 Protocol	The IPv6 network protocol being used. The options are dhcp | none.

Term	Definition
DHCPv6 Client DUID	The DHCPv6 client's unique client identifier. This row is displayed only when the configured IPv6 protocol is dhcp.
IPv6 Autoconfig Mode	Whether IPv6 Stateless address autoconfiguration is enabled or disabled.
Management VLAN	The VLAN used to establish an IP connection to the switch from a workstation that is connected to a port in the same VLAN.

The following shows example CLI display output for the network port.

```
(CN1610) #show network

Interface Status.............................. Down
IP Address.................................... 0.0.0.0
Subnet Mask................................... 0.0.0.0
Default Gateway............................... 0.0.0.0
IPv6 Administrative Mode...................... Enabled
Burned In MAC Address......................... 00:A0:98:EA:2E:7A
Locally Administered MAC address.............. 00:00:00:00:00:00
MAC Address Type.............................. Burned In
Configured IPv4 Protocol...................... None
Configured IPv6 Protocol...................... None
IPv6 AutoConfig Mode.......................... Disabled
Management VLAN ID............................ 1
```

show serviceport

This command displays service port configuration information.

Format	`show serviceport`
Mode	◆ Privileged EXEC ◆ User EXEC

Term	Definition
Interface Status	The network interface status. It is always considered to be up.
IP Address	The IP address of the interface. The factory default value is 0.0.0.0.
Subnet Mask	The IP subnet mask for this interface. The factory default value is 0.0.0.0.
Default Gateway	The default gateway for this IP interface. The factory default value is 0.0.0.0.
IPv6 Administrative Mode	Whether enabled or disabled. Default value is enabled.
IPv6 Prefix is	The IPv6 address and length. Default is Link Local format.
Configured IPv4 Protocol	The IPv4 network protocol being used. The options are bootp | dhcp | none.
Configured IPv6 Protocol	The IPv6 network protocol being used. The options are dhcp | none.
DHCPv6 Client DUID	The DHCPv6 client's unique client identifier. This row is displayed only when the configured IPv6 protocol is dhcp.
IPv6 Autoconfig Mode	Whether IPv6 Stateless address autoconfiguration is enabled or disabled.
Burned in MAC Address	The burned in MAC address used for in-band connectivity.

The following shows example CLI display output for the service port.

```
(CN1610) #show serviceport

Interface Status.............................. Up
IP Address.................................... 10.27.21.176
Subnet Mask................................... 255.255.252.0
Default Gateway............................... 10.27.20.1
IPv6 Administrative Mode...................... Enabled
```

```
IPv6 Prefix is ..............................
fe80::2a0:98ff:feea:2e7b/64
Configured IPv4 Protocol..................... DHCP
Configured IPv6 Protocol..................... None
IPv6 AutoConfig Mode......................... Disabled
Burned In MAC Address........................ 00:A0:98:EA:2E:7B
```

Console Port Access Commands

This section describes the commands you use to configure the console port. You can use a serial cable to connect a management host directly to the console port of the switch.

configure

This command gives you access to the Global Config mode. From the Global Config mode, you can configure a variety of system settings, including user accounts. From the Global Config mode, you can enter other command modes, including Line Config mode.

Format	`configure`
Mode	Privileged EXEC

line

This command gives you access to the Line Console mode, which allows you to configure various Telnet settings and the console port, as well as to configure console login/enable authentication.

Format	`line {console | telnet | ssh}`
Mode	Global Config

Term	Definition
console	Console terminal line.
telnet	Virtual terminal for remote console access (Telnet).
ssh	Virtual terminal for secured remote console access (SSH).

The following shows an example of the CLI command.

```
(CN1610)(config)#line telnet
(CN1610)(config-telnet)#
```

serial baudrate

This command specifies the communication rate of the terminal interface. The supported rates are 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200.

Default	9600
Format	`serial baudrate {1200 | 2400 | 4800 | 9600 | 19200 | 38400 | 57600 | 115200}`
Mode	Line Config

no serial baudrate

This command sets the communication rate of the terminal interface.

Format	`no serial baudrate`
Mode	Line Config

serial timeout

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

Default	5
Format	`serial timeout` *`0-160`*
Mode	Line Config

no serial timeout

This command sets the maximum connect time (in minutes) without console activity.

Format	`no serial timeout`
Mode	Line Config

show serial

This command displays serial communication settings for the switch.

Format	`show serial`

Modes	◆ Privileged EXEC ◆ User EXEC

Term	Definition
Serial Port Login Timeout (minutes)	The time, in minutes, of inactivity on a serial port connection, after which the switch will close the connection. A value of 0 disables the timeout.
Baud Rate (bps)	The default baud rate at which the serial port will try to connect.
Character Size (bits)	The number of bits in a character. The number of bits is always 8.
Flow Control	Whether Hardware Flow-Control is enabled or disabled. Hardware Flow Control is always disabled.
Stop Bits	The number of Stop bits per character. The number of Stop bits is always 1.
Parity	The parity method used on the Serial Port. The Parity Method is always None.

Telnet Commands

This section describes the commands you use to configure and view Telnet settings. You can use Telnet to manage the device from a remote management host.

ip telnet server enable

Use this command to enable Telnet connections to the system and to enable the Telnet Server Admin Mode. This command opens the Telnet listening port.

Default	enabled
Format	`ip telnet server enable`
Mode	Privileged EXEC

no ip telnet server enable

Use this command to disable Telnet access to the system and to disable the Telnet Server Admin Mode. This command closes the Telnet listening port and disconnects all open Telnet sessions.

Format	`no ip telnet server enable`
Mode	Privileged EXEC

telnet

This command establishes a new outbound Telnet connection to a remote host. The *host* value must be a valid IP address or host name. Valid values for *port* should be a valid decimal integer in the range of 0 to 65535, where the default value is 23. If *`[debug]`* is used, the current Telnet options enabled is displayed. The optional *line* parameter sets the outbound Telnet operational mode as linemode where, by default, the operational mode is character mode. The *localecho* option enables local echo.

Format	`telnet` *`ip-address|hostname port`* `[debug] [line] [localecho]`
Modes	◆ Privileged EXEC ◆ User EXEC

transport input telnet

This command regulates new Telnet sessions. If enabled, new Telnet sessions can be established until there are no more sessions available. An established session remains active until the session is ended or an abnormal network error ends the session.

Note

If the Telnet Server Admin Mode is disabled, Telnet sessions cannot be established. Use the `ip telnet server enable` command to enable Telnet Server Admin Mode.

Default	enabled
Format	`transport input telnet`
Mode	Line Config

no transport input telnet

Use this command to prevent new Telnet sessions from being established.

Format	`no transport input telnet`
Mode	Line Config

transport output telnet

This command regulates new outbound Telnet connections. If enabled, new outbound Telnet sessions can be established until the system reaches the maximum number of simultaneous outbound Telnet sessions allowed. An established session remains active until the session is ended or an abnormal network error ends it.

Default	enabled
Format	`transport output telnet`
Mode	Line Config

no transport output telnet

Use this command to prevent new outbound Telnet connection from being established.

Format	`no transport output telnet`
Mode	Line Config

session-limit

This command specifies the maximum number of simultaneous outbound Telnet sessions. A value of 0 indicates that no outbound Telnet session can be established.

Default	5
Format	`session-limit` *`0-5`*
Mode	Line Config

no session-limit

This command sets the maximum number of simultaneous outbound Telnet sessions to the default value.

Format	`no session-limit`
Mode	Line Config

session-timeout

This command sets the Telnet session timeout value.The timeout value unit of time is minutes.

Default	5
Format	`session-timeout` *`1-160`*
Mode	Line Config

no session-timeout

This command sets the Telnet session timeout value to the default. The timeout value unit of time is minutes.

Format	`no session-timeout`
Mode	Line Config

telnetcon maxsessions

This command specifies the maximum number of Telnet connection sessions that can be established. A value of 0 indicates that no Telnet connection can be established. The range is 0-5.

Default	5

Format	`telnetcon maxsessions` *`0-5`*
Mode	Privileged EXEC

no telnetcon maxsessions

This command sets the maximum number of Telnet connection sessions that can be established to the default value.

Format	`no telnetcon maxsessions`
Mode	Privileged EXEC

telnetcon timeout

This command sets the Telnet connection session timeout value, in minutes. A session is active as long as the session has not been idle for the value set. The time is a decimal value from 1 to 160.

Note

When you change the timeout value, the new value is applied to all active and inactive sessions immediately. Any sessions that have been idle longer than the new timeout value are disconnected immediately.

Default	5
Format	`telnetcon timeout` *`1-160`*
Mode	Privileged EXEC

no telnetcon timeout

This command sets the Telnet connection session timeout value to the default.

Note

Changing the timeout value for active sessions does not become effective until the session is accessed again. Also, any keystroke activates the new timeout duration.

Format	`no telnetcon timeout`
Mode	Privileged EXEC

show telnet

This command displays the current outbound Telnet settings. In other words, these settings apply to Telnet connections initiated from the switch to a remote system.

Format	`show telnet`
Modes	◆ Privileged EXEC ◆ User EXEC

Term	Definition
Outbound Telnet Login Timeout	The number of minutes an outbound Telnet session is allowed to remain inactive before being logged off.
Maximum Number of Outbound Telnet Sessions	The number of simultaneous outbound Telnet connections allowed.
Allow New Outbound Telnet Sessions	Indicates whether outbound Telnet sessions will be allowed.

show telnetcon

This command displays the current inbound Telnet settings. In other words, these settings apply to Telnet connections initiated from a remote system to the switch.

Format	`show telnetcon`
Modes	◆ Privileged EXEC ◆ User EXEC

Term	Definition
Remote Connection Login Timeout (minutes)	This object indicates the number of minutes a remote connection session is allowed to remain inactive before being logged off. May be specified as a number from 1 to 160. The factory default is 5.
Maximum Number of Remote Connection Sessions	This object indicates the number of simultaneous remote connection sessions allowed. The factory default is 5.

Term	Definition
Allow New Telnet Sessions	New Telnet sessions will not be allowed when this field is set to no. The factory default value is yes.
Telnet Server Admin Mode	The administrative mode of the telnet server.
Telnet Server Port	The TCP port number where the telnet server is listening.

The following output shows an example of the command:

```
(CN1610) #show telnetcon

Remote Connection Login Timeout (minutes)...... 5
Maximum Number of Remote Connection Sessions... 5
Allow New Telnet Sessions..................... Yes
Telnet Server Admin Mode...................... Enable
Telnet Server Port............................ 23
```

Secure Shell Commands

This section describes the commands you use to configure Secure Shell (SSH) access to the switch. Use SSH to access the switch from a remote management host.

Note
The system allows a maximum of 5 SSH sessions.

ip ssh

Use this command to enable SSH access to the system. (This command is the short form of the `ip ssh server enable` command.)

Default	disabled
Format	`ip ssh`
Mode	Privileged EXEC

ip ssh protocol

This command is used to set or remove protocol levels (or versions) for SSH. Either SSH1 (1), SSH2 (2), or both SSH 1 and SSH 2 (1 and 2) can be set.

Default	2
Format	`ip ssh protocol [1] [2]`
Mode	Privileged EXEC

ip ssh server enable

This command enables the IP secure shell server. No new SSH connections are allowed, but the existing SSH connections continue to work until timed-out or logged-out.

Default	enabled
Format	`ip ssh server enable`
Mode	Privileged EXEC

no ip ssh server enable

This command disables the IP secure shell server.

Format	`no ip ssh server enable`
Mode	Privileged EXEC

sshcon maxsessions

This command specifies the maximum number of SSH connection sessions that can be established. A value of 0 indicates that no ssh connection can be established. The range is 0 to 5.

Default	5
Format	`sshcon maxsessions` *`0-5`*
Mode	Privileged EXEC

no sshcon maxsessions

This command sets the maximum number of allowed SSH connection sessions to the default value.

Format	`no sshcon maxsessions`
Mode	Privileged EXEC

sshcon timeout

This command sets the SSH connection session timeout value, in minutes. A session is active as long as the session has been idle for the value set. The time is a decimal value from 1 to 160.

Changing the timeout value for active sessions does not become effective until the session is re accessed. Also, any keystroke activates the new timeout duration.

Default	5
Format	`sshcon timeout` *`1-160`*
Mode	Privileged EXEC

no sshcon timeout

This command sets the SSH connection session timeout value, in minutes, to the default.

Changing the timeout value for active sessions does not become effective until the session is re accessed. Also, any keystroke activates the new timeout duration.

Format	`no sshcon timeout`
Mode	Privileged EXEC

show ip ssh

This command displays the ssh settings.

Format	`show ip ssh`
Mode	Privileged EXEC

Term	Definition
Administrative Mode	This field indicates whether the administrative mode of SSH is enabled or disabled.
SSH port	The TCP port where the SSH server is listening
Protocol Level	The protocol level may have the values of version 1, version 2 or both versions 1 and version 2.
SSH Sessions Currently Active	The number of SSH sessions currently active.
Max SSH Sessions Allowed	The maximum number of SSH sessions allowed.
SSH Timeout	The SSH timeout value in minutes.
Keys Present	Indicates whether the SSH RSA and DSA key files are present on the device.
Key Generation in Progress	Indicates whether RSA or DSA key files generation is currently in progress.

Management Security Commands

This section describes commands you use to generate keys and certificates, which you can do in addition to loading them as before.

crypto key generate rsa

Use this command to generate an RSA key pair for SSH. The new key files will overwrite any existing generated or downloaded RSA key files.

Format	`crypto key generate rsa`
Mode	Global Config

no crypto key generate rsa

Use this command to delete the RSA key files from the device.

Format	`no crypto key generate rsa`
Mode	Global Config

crypto key generate dsa

Use this command to generate a DSA key pair for SSH. The new key files will overwrite any existing generated or downloaded DSA key files.

Format	`crypto key generate dsa`
Mode	Global Config

no crypto key generate dsa

Use this command to delete the DSA key files from the device.

Format	`no crypto key generate dsa`
Mode	Global Config

Access Commands

Use the commands in this section to close remote connections or to view information about connections to the system.

disconnect

Use the `disconnect` command to close Telnet or SSH sessions. Use `all` to close all active sessions, or use *`session-id`* to specify the session ID to close. To view the possible values for *`session-id`*, use the `show loginsession` command.

Format	`disconnect {`*`session_id`*` | all}`
Mode	Privileged EXEC

linuxsh

Use the `linuxsh` command to access the Linux shell. Use the `exit` command to exit the Linux shell and return to the CN1610 CLI. The shell session will timeout after five minutes of inactivity. The inactivity timeout value can be changed using the command "session-timeout" on page 43 in Line Console mode.

Default	ip-port:2324
Format	`linuxsh [`*`ip-port`*`]`
Mode	Privileged EXEC

Parameter	Description
ip-port	The IP port number on which the telnet daemon listens for connections. ip-port is an integer from 1 to 65535. The default value is 2324.

show loginsession

This command displays current Telnet, SSH and serial port connections to the switch. This command displays truncated user names. Use the `show loginsession long` command to display the complete usernames.

Format	`show loginsession`

Mode	Privileged EXEC

Term	Definition
ID	Login Session ID.
User Name	The name the user entered to log on to the system.
Connection From	IP address of the remote client machine or EIA-232 for the serial port connection.
Idle Time	Time this session has been idle.
Session Time	Total time this session has been connected.
Session Type	Shows the type of session, which can be telnet, serial, or SSH.

show loginsession long

This command displays the complete user names of the users currently logged in to the switch.

Format	`show loginsession long`
Mode	Privileged EXEC

The following shows an example of the command.

```
(CN1610) #show loginsession long
User Name
------------
admin
test1111test1111test1111test1111test1111test1111test1111test1111
```

User Account Commands

This section describes the commands you use to add, manage, and delete system users. FASTPATH software has two default users: admin and guest. The admin user can view and configure system settings, and the guest user can view settings.

Note
You cannot delete the admin user. There is only one user allowed with level-15 privileges. You can configure up to five level-1 users on the system.

aaa authentication login

Use this command to set authentication at login. The default and optional list names created with the command are used with the `aaa authentication login` command. Create a list by entering the `aaa authentication login list-name method` command, 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 there is an authentication failure. To ensure that the authentication succeeds even if all methods return an error, specify `none` as the fInal method in the command line. For example, if `none` is specified as an authentication method after `radius`, no authentication is used if the RADIUS server is down.

Default	◆ `defaultList`. Used by the console and only contains the method none. ◆ `networkList`. Used by telnet and SSH and only contains the method local.
Format	`aaa authentication login {default | list-name} method1 [method2...]`
Mode	Global Config

Parameter	Definition
default	Uses the listed authentication methods that follow this argument as the default list of methods when a user logs in.

Parameter	Definition
list-name	Character string of up to 15 characters used to name the list of authentication methods activated when a user logs in.
method1... *[*method2...*]*	At least one from the following: ◆ enable. Uses the enable password for authentication. ◆ line. Uses the line password for authentication. ◆ local. Uses the local username database for authentication. ◆ none. Uses no authentication. ◆ radius. Uses the list of all RADIUS servers for authentication. ◆ tacacs. Uses the list of all TACACS servers for authentication.

The following shows an example of the command.

```
(CN1610)(config)# aaa authentication login default radius local
enable none
```

no aaa authentication login

This command returns to the default.

Format	`aaa authentication login {default | list-name}`
Mode	Global Config

aaa authentication enable

Use this command to set authentication for accessing higher privilege levels. The default enable list is `enableList`. It is used by console, and contains the method as `enable` followed by `none`.

A separate default enable list, enableNetList, is used for Telnet and SSH users instead of enableList. This list is applied by default for Telnet and SSH, and contains enable followed by deny methods. In CN1610, by default, the enable password is not configured. That means that, by default, Telnet and SSH users

will not get access to Privileged EXEC mode. On the other hand, with default conditions, a console user always enter the Privileged EXEC mode without entering the enable password.

The default and optional list names created with the `aaa authentication enable` command are used with the `enable authentication` command. Create a list by entering the `aaa authentication enable list-name method` command 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 user manager returns ERROR (not PASS or FAIL) for enable and line methods if no password is configured, and moves to the next configured method in the authentication list. The method `none` reflects that there is no authentication needed.

The user will only be prompted for an enable password if one is required. The following authentication methods do not require passwords:

1. none
2. deny
3. enable (if no enable password is configured)
4. line (if no line password is configured)

See the examples below.

- `aaa authentication enable default enable none`
- `aaa authentication enable default line none`
- `aaa authentication enable default enable radius none`
- `aaa authentication enable default line tacacs none`

The first two examples do not prompt for a password; however, because the last two examples contain the `radius` and `tacacs` methods, the password prompt is displayed.

If the login methods include only enable, and there is no enable password configured, then CN1610 does not prompt for a username. In such cases, CN1610 only prompts for a password. CN1610 supports configuring methods after the local method in authentication and authorization lists. If the user is not present in the local database, then the next configured method is tried.

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.

Use the command "show authorization methods" on page 59 to display information about the authentication methods.

Note

Requests sent by the switch to a RADIUS server include the username `$enabx$`, where *x* is the requested privilege level. For enable to be authenticated on Radius servers, add `$enabx$` users to them. The login user ID is now sent to TACACS+ servers for enable authentication.

Default	default
Format	`aaa authentication enable {default | list-name} method1 [method2...]`
Mode	Global Config

Parameter	Description
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: 1-15 characters.
method1 *[*method2...*]*	Specify at least one from the following: ◆ `deny`. Used to deny access. ◆ `enable`. Uses the enable password for authentication. ◆ `line`. Uses the line password for authentication. ◆ `none`. Uses no authentication. ◆ `radius`. Uses the list of all RADIUS servers for authentication. ◆ `tacacs`. Uses the list of all TACACS+ servers for authentication.

The following example sets authentication when accessing higher privilege levels.

```
(CN1610)(config)# aaa authentication enable default enable
```

no aaa authentication enable

Use this command to return to the default configuration.

Format	`no aaa authentication enable {default | list-name}`
Mode	Global Config

aaa authorization

Use this command to configure an exec authorization method list. This list is identified by `default` or a user-specified *`list-name`*. If `tacacs` is specified as the authorization method, authorization commands are notified to a TACACS+ server.

Exec Authorization

When exec authorization is configured for a line mode, the user may not be required to use the enable command to enter Privileged EXEC mode. If the authorization response indicates that the user has sufficient privilege levels for Privileged EXEC mode, then the user bypasses User EXEC mode entirely.

The exec authorization usage scenario is this:

1. Configure Authorization Method List

   `aaa authorization exec` *`listname method1`* `[`*`method2....`*`]`

2. Apply AML to an Access Line Mode (console, telnet, SSH)

   `authorization exec` *`listname`*

3. When the user logs in, in addition to authentication, authorization will be performed to determine if the user is allowed direct access to Privileged EXEC mode.

Format	`aaa authorization exec {default|`*`list-name`*`}` *`method1`*`[`*`method2`*`]`
Mode	Global Config

Parameter	Description
exec	Provides exec authorization.
default	The default list of methods for authorization services.

Parameter	Description
list-name	Alphanumeric character string used to name the list of authorization methods.
method	`TACACS+/RADIUS/Local` and `none` are supported.

The following shows an example of the command.

```
(CN1610) #
(CN1610) #configure
(CN1610) (Config)#aaa authorization exec default  tacacs+ none
```

no aaa authorization

This command deletes the authorization method list.

Format	`no aaa authorization commands {default|list-name}`
Mode	Global Config

authorization exec

This command applies a command authorization method list to an access method so that the user may not be required to use the enable command to enter Privileged EXEC mode. For usage scenarios on exec authorization, see the command “aaa authorization” on page 57.

Format	`authorization exec list-name`
Mode	Line console, Line telnet, Line SSH

Parameter	Description
list-name	The command authorization method list.

no authorization exec

This command removes command authorization from a line config mode.

Format	`no authorization exec`
Mode	Line console, Line telnet, Line SSH

authorization exec default

This command applies a default command authorization method list to an access method so that the user may not be required to use the enable command to enter Privileged EXEC mode. For usage scenarios on exec authorization, see the command "aaa authorization" on page 57.

Format	`authorization exec default`
Mode	Line console, Line telnet, Line SSH

no authorization exec default

This command removes command authorization from a line config mode.

Format	`no authorization exec default`
Mode	Line console, Line telnet, Line SSH

show authorization methods

This command displays the configured authorization method lists.

Format	`show authorization methods`
Mode	Privileged EXEC

The following shows example CLI display output for the command.

```
(CN1610) #show authorization methods

Exec Authorization Method Lists
-----------------------------------
dfltExecAuthList               :      none

Line       Exec Method List
---------  --------------------
Console    dfltExecAuthList
Telnet     dfltExecAuthList
SSH        dfltExecAuthList
```

enable authentication

Use this command to specify the authentication method list when accessing a higher privilege level from a remote telnet or console.

Format	`enable authentication {default | list-name}`

Mode	Line Config

Parameter	Description
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.

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

```
(CN1610)(config)# line console
(CN1610)(config-line)# enable authentication default
```

no enable authentication

Use this command to return to the default specified by the `enable authentication` command.

Format	`no enable authentication`
Mode	Line Config

username (Global Config)

Use the `username` command in Global Config mode to add a new user to the local user database. The default privilege level is 1. Using the `encrypted` keyword allows the administrator to transfer local user passwords between devices without having to know the passwords. When the `password` parameter is used along with `encrypted` parameter, the password must be exactly 128 hexadecimal characters in length. If the password strength feature is enabled, this command checks for password strength and returns an appropriate error if it fails to meet the password strength criteria. Giving the optional parameter `override-complexity-check` disables the validation of the password strength.

Format	`username` *`name`* {`password` *`password`* `[encrypted [override-complexity-check] | level` *`level`* `[encrypted [override-complexity-check]] | override-complexity-check]} | {level` *`level`* `[override-complexity-check] password}`
Mode	Global Config

Parameter	Description
name	The name of the user. Range: 1-64 characters.
password	The authentication password for the user. Range 8-64 characters. This value can be zero if the `no passwords min-length` command has been executed. The special characters allowed in the password include ! # $ % & ' ( ) * + , - . / : ; < = > @ [\ ] ^ _ ` { | } ~.
level	The user level. Level 0 can be assigned by a level 15 user to another user to suspend that user's access. Range 0-15. Enter access level 1 for non-privileged (switch> prompt) or 15 for highest privilege (switch# prompt) Access. If not specified where it is optional, the privilege level is 1.
encrypted	Encrypted password entered, copied from another switch configuration.
override-complexity-check	Disables the validation of the password strength.

The following example configures user `bob` with password `xxxyyymmmm` and user level 15.

```
(CN1610)(config)# username bob password xxxyyymmmm level 15
```

The following example configures user test with password testPassword and assigns a user level of 1. The password strength will not be validated.

```
(CN1610)(config)# username test password testPassword level 1
override-complexity-check
```

A third example.

```
(Switching) (Config)#username test password testtest
```

A fourth example.

```
(Switching) (Config)# username test password
e8d63677741431114f9e39a853a15e8fd35ad059e2e1b49816c243d7e08152b052
eafbf23b528d348cdba1b1b7ab91be842278e5e970dbfc62d16dcd13c0b864
level 1 encrypted override-complexity-check
```

```
(Switching) (Config)#  username test level 15 password

Enter new password:********

Confirm new password:********
```

A fifth example.

```
(Switching) (Config)# username test level 15 override-complexity-
check  password

Enter new password:********

Confirm new password:********
```

no username

Use this command to remove a user name.

Format	`no username` *`name`*
Mode	Global Config

username nopassword

Use this command to remove an existing user's password (NULL password).

Format	`username` *`name`* `nopassword` *`[level level]`*
Mode	Global Config

Parameter	Description
name	The name of the user. Range: 1-32 characters.
password	The authentication password for the user. Range 8-64 characters.
level	The user level. Level 0 can be assigned by a level 15 user to another user to suspend that user's access. Range 0-15.

username unlock

Use this command to allows a locked user account to be unlocked. Only a user with Level 1 access can reactivate a locked user account.

Format	`username` *`name`* `unlock`
Mode	Global Config

username snmpv3 accessmode

This command specifies the snmpv3 access privileges for the specified login user. The valid accessmode values are `readonly` or `readwrite`. The *`username`* is the login user name for which the specified access mode applies. The default is `readwrite` for the "admin" user and `readonly` for all other users. You must enter the *`username`* in the same case you used when you added the user. To see the case of the *`username`*, enter the `show users` command.

Defaults	◆ admin - readwrite ◆ other - readonly
Format	`username snmpv3 accessmode` *`username`* {*`readonly`* | *`readwrite`*}
Mode	Global Config

no username snmpv3 accessmode

This command sets the snmpv3 access privileges for the specified user as **readwrite** for the "admin" user and **readonly** for all other users. The *`username`* value is the user name for which the specified access mode will apply.

Format	`no username snmpv3 accessmode` *`username`*
Mode	Global Config

username snmpv3 authentication

This command specifies the authentication protocol to be used for the specified user. The valid authentication protocols are `none`, `md5` or `sha`. If you specify `md5` or `sha`, the login password is also used as the snmpv3 authentication password and therefore must be at least eight characters in length. The *`username`* is the user name associated with the authentication protocol. You must enter the *`username`* in the same case you used when you added the user. To see the case of the *`username`*, enter the `show users` command.

Default	no authentication
Format	`username snmpv3 authentication` *`username`* {`none` | `md5` | `sha`}
Mode	Global Config

no username snmpv3 authentication

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

Format	`no username snmpv3 authentication` *`username`*
Mode	Global Config

username snmpv3 encryption

This command specifies the encryption protocol used for the specified user. The valid encryption protocols are `des` or `none`.

If you select `des`, you can specify the required key on the command line. The encryption key must be 8 to 64 characters long. If you select the `des` protocol but do not provide a key, the user is prompted for the key. When you use the `des` protocol, the login password is also used as the snmpv3 encryption password, so it must be a minimum of eight characters. If you select `none`, you do not need to provide a key.

The *`username`* value is the login user name associated with the specified encryption. You must enter the *`username`* in the same case you used when you added the user. To see the case of the *`username`*, enter the `show users` command.

Default	no encryption
Format	`username snmpv3 encryption` *`username`* {`none` | `des` *`[key]`*}
Mode	Global Config

no username snmpv3 encryption

This command sets the encryption protocol to **none**. The *username* is the login user name for which the specified encryption protocol will be used.

Format	`no username snmpv3 encryption` *username*
Mode	Global Config

username snmpv3 encryption encrypted

This command specifies the des encryption protocol and the required encryption key for the specified user. The encryption key must be 8 to 64 characters long.

Default	no encryption
Format	`username snmpv3 encryption encrypted` *username* `des` *key*
Mode	Global Config

show users

This command displays the configured user names and their settings. The `show users` command displays truncated user names. Use the `show users long` command to display the complete usernames. The `show users` command is only available for users with Level 15 privileges. The SNMPv3 fields will only be displayed if SNMP is available on the system.

Format	`show users`
Mode	Privileged EXEC

Term	Definition
User Name	The name the user enters to login using the serial port, SSH, or Telnet.
Access Mode	Shows whether the user is able to change parameters on the switch (Level 15) or is only able to view them (Level 1). As a factory default, the “admin” user has Level 15 access and the “guest” has Level 1 access.

Term	Definition
SNMPv3 Access Mode	The SNMPv3 Access Mode. If the value is set to `ReadWrite`, the SNMPv3 user is able to set and retrieve parameters on the system. If the value is set to `ReadOnly`, the SNMPv3 user is only able to retrieve parameter information. The SNMPv3 access mode may be different than the CLI access mode.
SNMPv3 Authentication	The authentication protocol to be used for the specified login user.
SNMPv3 Encryption	The encryption protocol to be used for the specified login user.

show users long

This command displays the complete usernames of the configured users on the switch.

Format	`show users long`
Mode	Privileged EXEC

The following shows an example of the command.

```
(CN1610) #show users long
User Name
------------
admin
guest
test1111test1111test1111test1111
```

show users accounts

This command displays the local user status with respect to user account lockout and password aging.This command displays truncated user names. Use the `show users long` command to display the complete usernames.

Format	`show users accounts [detail]`
Mode	Privileged EXEC

Term	Definition
User Name	The local user account's user name.
Access Level	The user's access level (1 for non-privilege (switch>prompt) or 15 for highest privilege (switch# prompt).
Password Aging	Number of days, since the password was configured, until the password expires.
Password Expiry Date	The current password expiration date in date format.
Lockout	Indicates whether the user account is locked out (true or false).

If the detail keyword is included, the following additional fields display.

Term	Definition
Password Override Complexity Check	Displays the user's Password override complexity check status. By default it is disabled.
Password Strength	Displays the user password's strength (Strong or Weak). This field is displayed only if the Password Strength feature is enabled.

The following example displays information about the local user database.

```
(CN1610)#show users accounts

UserName            Privilege Password Password     Lockout
                              Aging    Expiry date
------------------- --------- -------- ------------ -------
admin               15        ---      ---          False
guest               1         ---      ---          False

console#show users accounts detail

UserName..................................... admin
Privilege.................................... 15
Password Aging............................... ---
Password Expiry.............................. ---
```

```
Lockout..................................... False
Override Complexity Check................... Disable
Password Strength........................... ---

UserName.................................... guest
Privilege................................... 1
Password Aging.............................. ---
Password Expiry............................. ---
Lockout..................................... False
Override Complexity Check................... Disable
Password Strength........................... ---
```

show users login-history [long]

Use this command to display information about the login history of users.

Format	`show users login-history [long]`
Mode	Privileged EXEC

show users login-history [username]

Use this command to display information about the login history of users.

Format	`show users login-history [username` *`name`*`]`
Mode	Privileged EXEC

Parameter	Description
name	Name of the user. Range: 1-20 characters.

The following example shows user login history outputs.

```
Console>show users login-history
Login Time           Username  Protocol  Location
-------------------  --------- --------- ---------------
Jan 19 2005 08:23:48  Bob       Serial
Jan 19 2005 08:42:31  John      SSH       172.16.0.1
Jan 19 2005 08:49:52  Betty     Telnet    172.16.1.7
```

login authentication

Use this command to specify the login authentication method list for a line (console, telnet, or SSH). The default configuration uses the default set with the command `aaa authentication login`.

Format	`login authentication {default | list-name}`
Mode	Line Configuration

Parameter	Description
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.

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

```
(CN1610) (config)# line console
(CN1610) (config-line)# login authentication default
```

no login authentication

Use this command to return to the default specified by the `authentication login` command.

password

This command allows the currently logged in user to change his or her password without having Level 15 privileges.

Format	`password cr`
Mode	User EXEC

The following is an example of the command.

```
console>password

Enter old password:********

Enter new password:********

Confirm new password:********
```

password (Line Configuration)

Use the `password` command in Line Configuration mode to specify a password on a line. The default configuration is no password is specified.

Format	password [*password* [encrypted]]
Mode	Line Config

Parameter	Definition
password	Password for this level. Range: 8-64 characters
encrypted	Encrypted password to be entered, copied from another switch configuration. The encrypted password should be 128 characters long because the assumption is that this password is already encrypted with AES.

The following example specifies a password mcmxxyyy on a line.

```
(CN1610)(config-line)# password mcmxxyyy
```

The following is another example of the command.

```
(Switching)(Config-line)# password testtest

(Switching) (Config-line)# password
e8d636777414311l4f9e39a853a15e8fd35ad059e2e1b49816c243d7e08152b052
eafbf23b528d348cdba1b1b7ab91be842278e5e970dbfc62d16dcd13c0b864
encrypted

(Switching) (Config-line)# password

Enter new password:********

Confirm new password:********
```

no password (Line Configuration)

Use this command to remove the password on a line.

Format	no password
Mode	Line Config

password (User EXEC)

Use this command to allow a user to change the password for only that user. This command should be used after the password has aged. The user is prompted to enter the old password and the new password.

Format	`password`
Mode	User EXEC

The following example shows the prompt sequence for executing the password command.

```
(CN1610)>password
Enter old password:********
Enter new password:********
Confirm new password:********
```

password (aaa IAS User Config)

This command is used to configure a password for a user. An optional parameter [encrypted] is provided to indicate that the password given to the command is already preencrypted.

Format	`password` *`password`* `[encrypted]`
Mode	aaa IAS User Config

no password (aaa IAS User Config)

This command is used to clear the password of a user.

Format	`no password`
Mode	aaa IAS User Config

The following shows an example of the command.

```
(CN1610) #
(CN1610) #configure
(CN1610) (Config)#aaa ias-user username client-1
(CN1610) (Config-aaa-ias-User)#password client123
(CN1610) (Config-aaa-ias-User)#no password
```

The following is an example of adding a MAB Client to the Internal user database.

```
(CN1610) #
```

```
(CN1610) #configure
(CN1610) (Config)#aaa ias-user username 1f3ccb1157
(CN1610) (Config-aaa-ias-User)#password 1f3ccb1157
(CN1610) (Config-aaa-ias-User)#exit
(CN1610) (Config)#
```

enable password (Privileged EXEC)

Use the `enable password` configuration command to set a local password to control access to the privileged EXEC mode.

Format	`enable password [`*`password`* `[encrypted]]`
Mode	Privileged EXEC

Parameter	Description
password	Password string. Range: 8-64 characters.
encrypted	Encrypted password you entered, copied from another switch configuration. The encrypted password should be 128 characters long because the assumption is that this password is already encrypted with AES.

The following shows an example of the command.

```
(Switching) #enable password testtest

(Switching) #enable password
e8d63677741431114f9e39a853a15e8fd35ad059e2e1b49816c243d7e08152b052
eafbf23b528d348cdba1b1b7ab91be842278e5e970dbfc62d16dcd13c0b864
encrypted

(Switching) #enable password

Enter old password:********

Enter new password:********

Confirm new password:********
```

no enable password (Privileged EXEC)

Use the `no enable password` command to remove the password requirement.

Format	`no enable password`
Mode	Privileged EXEC

passwords min-length

Use this command to enforce a minimum password length for local users. The value also applies to the enable password. The valid range is 8-64.

Default	8
Format	`passwords min-length` *`8-64`*
Mode	Global Config

no passwords min-length

Use this command to set the minimum password length to the default value.

Format	`no passwords min-length`
Mode	Global Config

passwords history

Use this command to set the number of previous passwords that shall be stored for each user account. When a local user changes his or her password, the user will not be able to reuse any password stored in password history. This ensures that users don't reuse their passwords often. The valid range is 0-10.

Default	0
Format	`passwords history` *`0-10`*
Mode	Global Config

no passwords history

Use this command to set the password history to the default value.

Format	`no passwords history`
Mode	Global Config

passwords aging

Use this command to implement aging on passwords for local users. When a user's password expires, the user will be prompted to change it before logging in again. The valid range is 1-365. The default is 0, or no aging.

Default	0
Format	`passwords aging` *`1-365`*
Mode	Global Config

no passwords aging

Use this command to set the password aging to the default value.

Format	`no passwords aging`
Mode	Global Config

passwords lock-out

Use this command to strengthen the security of the switch by locking user accounts that have failed login due to wrong passwords. When a lockout count is configured, a user that is logged in must enter the correct password within that count. Otherwise the user will be locked out from further switch access. Only a user with Level 15 access can reactivate a locked user account. Password lockout does not apply to logins from the serial console. The valid range is 1-5. The default is 0, or no lockout count enforced.

Default	0
Format	`passwords lock-out` *`1-5`*
Mode	Global Config

no passwords lock-out

Use this command to set the password lock-out count to the default value.

Format	`no passwords lock-out`
Mode	Global Config

passwords strength-check

Use this command to enable the password strength feature. It is used to verify the strength of a password during configuration.

Default	Disable
Format	`passwords strength-check`
Mode	Global Config

no passwords strength-check

Use this command to set the password strength checking to the default value.

Format	`no passwords strength-check`
Mode	Global Config

passwords strength maximum consecutive-characters

Use this command to set the maximum number of consecutive characters to be used in password strength. The valid range is 0-15. The default is 0. Minimum of 0 means no restriction on that set of characters.

Default	0
Format	`passwords strength maximum consecutive-characters` *`0-15`*
Mode	Global Config

passwords strength maximum repeated-characters

Use this command to set the maximum number of repeated characters to be used in password strength. The valid range is 0-15. The default is 0. Minimum of 0 means no restriction on that set of characters.

Default	0
Format	`passwords strength maximum consecutive-characters` *`0-15`*
Mode	Global Config

passwords strength minimum uppercase-letters

Use this command to enforce a minimum number of uppercase letters that a password should contain. The valid range is 0-16. The default is 2. Minimum of 0 means no restriction on that set of characters.

Default	2
Format	`passwords strength minimum uppercase-letters`
Mode	Global Config

no passwords strength minimum uppercase-letters

Use this command to reset the minimum uppercase letters required in a password to the default value.

Format	`no passwords minimum uppercase-letter`
Mode	Global Config

passwords strength minimum lowercase-letters

Use this command to enforce a minimum number of lowercase letters that a password should contain. The valid range is 0-16. The default is 2. Minimum of 0 means no restriction on that set of characters.

Default	2
Format	`passwords strength minimum lowercase-letters`
Mode	Global Config

no passwords strength minimum lowercase-letters

Use this command to reset the minimum lower letters required in a password to the default value.

Format	`no passwords minimum lowercase-letter`
Mode	Global Config

passwords strength minimum numeric-characters

Use this command to enforce a minimum number of numeric characters that a password should contain. The valid range is 0-16. The default is 2. Minimum of 0 means no restriction on that set of characters.

Default	2
Format	`passwords strength minimum numeric-characters`
Mode	Global Config

no passwords strength minimum numeric-characters

Use this command to reset the minimum numeric characters required in a password to the default value.

Format	`no passwords minimum numeric-characters`
Mode	Global Config

passwords strength minimum special-characters

Use this command to enforce a minimum number of special characters that a password should contain. The valid range is 0-16. The default is 2. Minimum of 0 means no restriction on that set of characters.

Default	2
Format	`passwords strength minimum special-characters`
Mode	Global Config

no passwords strength minimum special-characters

Use this command to reset the minimum special characters required in a password to the default value.

Format	`no passwords minimum special-characters`
Mode	Global Config

passwords strength minimum character-classes

Use this command to enforce a minimum number of characters classes that a password should contain. Character classes are uppercase letters, lowercase letters, numeric characters and special characters. The valid range is 0-4. The default is 4.

Default	4
Format	`passwords strength minimum character-classes`
Mode	Global Config

no passwords strength minimum character-classes

Use this command to reset the minimum number of character classes required in a password to the default value.

Format	`no passwords minimum character-classes`
Mode	Global Config

passwords strength exclude-keyword

Use this command to exclude the specified keyword while configuring the password. The password does not accept the keyword in any form (in between the string, case in-sensitive and reverse) as a substring. User can configure up to a maximum of 3 keywords.

Format	`passwords strength exclude-keyword` *`keyword`*
Mode	Global Config

no passwords strength exclude-keyword

Use this command to reset the restriction for the specified keyword or all the keywords configured.

Format	`no passwords exclude-keyword` *`[keyword]`*
Mode	Global Config

show passwords configuration

Use this command to display the configured password management settings.

Format	`show passwords configuration`

Mode	Privileged EXEC

Term	Definition
Minimum Password Length	Minimum number of characters required when changing passwords.
Password History	Number of passwords to store for reuse prevention.
Password Aging	Length in days that a password is valid.
Lockout Attempts	Number of failed password login attempts before lockout.
Minimum Password Uppercase Letters	Minimum number of uppercase characters required when configuring passwords.
Minimum Password Lowercase Letters	Minimum number of lowercase characters required when configuring passwords.
Minimum Password Numeric Characters	Minimum number of numeric characters required when configuring passwords.
Maximum Password Consecutive Characters	Maximum number of consecutive characters required that the password should contain when configuring passwords.
Maximum Password Repeated Characters	Maximum number of repetition of characters that the password should contain when configuring passwords.
Minimum Password Character Classes	Minimum number of character classes (uppercase, lowercase, numeric and special) required when configuring passwords.
Password Exclude-Keywords	The set of keywords to be excluded from the configured password when strength checking is enabled.

show passwords result

Use this command to display the last password set result information.

Format	`show passwords result`

Mode	Privileged EXEC

Term	Definition
Last User Whose Password Is Set	Shows the name of the user with the most recently set password.
Password Strength Check	Shows whether password strength checking is enabled.
Last Password Set Result	Shows whether the attempt to set a password was successful. If the attempt failed, the reason for the failure is included.

aaa ias-user username

The Internal Authentication Server (IAS) database is a dedicated internal database used for local authentication of users for network access through the IEEE 802.1X feature.

Use the `aaa ias-user username` command in Global Config mode to add the specified user to the internal user database. This command also changes the mode to AAA User Config mode.

Format	`aaa ias-user username` *user*
Mode	Global Config

no aaa ias-user username

Use this command to remove the specified user from the internal user database.

Format	`no aaa ias-user username` *user*
Mode	Global Config

The following shows an example of the command.

```
(CN1610) #
(CN1610) #configure
(CN1610) (Config)#aaa ias-user username client-1
(CN1610) (Config-aaa-ias-User)#exit
(CN1610) (Config)#no aaa ias-user username client-1
(CN1610) (Config)#
```

aaa session-id

Use this command in Global Config mode to specify if the same session-id is used for Authentication, Authorization and Accounting service type within a session.

Default	`common`
Format	`aaa session-id [common | unique]`
Mode	Global Config

Parameter	Description
common	Use the same session-id for all AAA Service types.
unique	Use a unique session-id for all AAA Service types.

no aaa session-id

Use this command in Global Config mode to reset the aaa session-id behavior to the default.

Format	`no aaa session-id [unique]`
Mode	Global Config

aaa accounting

Use this command in Global Config mode to create an accounting method list for user EXEC sessions, user-executed commands, or DOT1X. This list is identified by **default** or a user-specified **list_name**. Accounting records, when enabled for a line-mode, can be sent at both the beginning and at the end (**start-stop**) or only at the end (**stop-only**). If **none** is specified, then accounting is disabled for the specified list. If **tacacs** is specified as the accounting method, accounting records are notified to a TACACS+ server. If **radius** is the specified accounting method, accounting records are notified to a RADIUS server.

Note

Note the following:

- A maximum of five Accounting Method lists can be created for each exec and commands type.
- Only the default Accounting Method list can be created for DOT1X. There is no provision to create more.

- The same list-name can be used for both exec and commands accounting type
- AAA Accounting for commands with RADIUS as the accounting method is not supported.
- Start-stop or None are the only supported record types for DOT1X accounting. Start-stop enables accounting and None disables accounting.
- RADIUS is the only accounting method type supported for DOT1X accounting.

Format	`aaa accounting {exec | commands | dot1x} {default | list_name} {start-stop | stop-only |none} method1 [method2…]`
Mode	Global Config

Parameter	**Description**
exec	Provides accounting for a user EXEC terminal sessions.
commands	Provides accounting for all user executed commands.
dot1x	Provides accounting for DOT1X user commands.
default	The default list of methods for accounting services.
list-name	Character string used to name the list of accounting methods.
start-stop	Sends a start accounting notice at the beginning of a process and a stop accounting notice at the beginning of a process and a stop accounting notice at the end of a process.
stop-only	Sends a stop accounting notice at the end of the requested user process.
none	Disables accounting services on this line.
method	Use either TACACS or radius server for accounting purposes.

The following shows an example of the command.

```
(CN1610) #
(CN1610) #configure
(CN1610) #aaa accounting commands default stop-only tacacs
(CN1610) #aaa accounting exec default start-stop radius
(CN1610) #aaa accounting dot1x default start-stop radius
(CN1610) #aaa accounting dot1x default none
(CN1610) #exit
```

For the same set of accounting type and list name, the administrator can change the record type, or the methods list, without having to first delete the previous configuration.

```
(CN1610) #
(CN1610) #configure
(CN1610) #aaa accounting exec ExecList stop-only tacacs
(CN1610) #aaa accounting exec ExecList start-stop tacacs
(CN1610) #aaa accounting exec ExecList start-stop tacacs radius
```

The first **aaa** command creates a method list for exec sessions with the name *ExecList*, with **record-type** as *stop-only* and the **method** as *TACACS+*. The second command changes the **record type** to *start-stop* from *stop-only* for the same method list. The third command, for the same list changes the **methods list** to {*tacacs,radius*} from {*tacacs*}.

no aaa accounting

This command deletes the accounting method list.

Format	`no aaa accounting {exec | commands | dot1x} {default | list_name default}`
Mode	Global Config

The following shows an example of the command.

```
(CN1610) #
(CN1610) #configure
(CN1610) #aaa accounting commands userCmdAudit stop-only tacacs
radius
(CN1610) #no aaa accounting commands userCmdAudit
(CN1610) #exit
```

password (AAA IAS User Configuration)

Use this command to specify a password for a user in the IAS database. An optional parameter **encrypted** is provided to indicate that the password given to the command is already preencrypted.

Format	password *password* [encrypted]
Mode	AAA IAS User Config

Parameter	Definition
password	Password for this level. Range: 8-64 characters
encrypted	Encrypted password to be entered, copied from another switch configuration.

no password (AAA IAS User Configuration)

Use this command to clear the password of a user.

Format	no password
Mode	AAA IAS User Config

The following shows an example of the command.

```
(CN1610) #
(CN1610) #configure
(CN1610) (Config)#aaa ias-user username client-1
(CN1610) (Config-aaa-ias-User)#password client123
(CN1610) (Config-aaa-ias-User)#no password
```

The following is an example of adding a MAB Client to the Internal user database.

```
(CN1610) #
(CN1610) #configure
(CN1610) (Config)#aaa ias-user username 1f3ccb1157
(CN1610) (Config-aaa-ias-User)#password 1f3ccb1157
(CN1610) (Config-aaa-ias-User)#exit
(CN1610) (Config)#
```

clear aaa ias-users

Use this command to remove all users from the IAS database.

Format	clear aaa ias-users
Mode	Privileged EXEC

Parameter	Definition
password	Password for this level. Range: 8-64 characters
encrypted	Encrypted password to be entered, copied from another switch configuration.

The following is an example of the command.

```
(CN1610) #
(CN1610) #clear aaa ias-users
(CN1610) #
```

show aaa ias-users

Use this command to display configured IAS users and their attributes. Passwords configured are not shown in the show command output.

Format	`show aaa ias-users [username]`
Mode	Privileged EXEC

The following is an example of the command.

```
(CN1610) #
(CN1610) #show aaa ias-users

UserName
------------------
Client-1
Client-2
```

Following are the IAS configuration commands shown in the output of show running-config command. Passwords shown in the command output are always encrypted.

```
aaa ias-user username client-1
password
a45c74fdf50a558a2b5cf05573cd633bac2c6c598d54497ad4c46104918f2c
encrypted
exit
```

accounting

Use this command in Line Configuration mode to apply the accounting method list to a line config (console/telnet/ssh).

Format	accounting {exec | commands } {default | *listname*}
Mode	Line Configuration

Parameter	Description
exec	Causes accounting for an EXEC session.
commands	This causes accounting for each command execution attempt. If a user is enabling accounting for exec mode for the current line-configuration type, the user will be logged out.
default	The default Accounting List
listname	Enter a string of not more than 15 characters.

The following is a example of the command.

```
(CN1610) #
(CN1610) #configure
(CN1610) (Config)#line telnet
(CN1610)(Config-line)# accounting exec default
(CN1610) #exit
```

no accounting

Use this command to remove accounting from a Line Configuration mode.

Format	no accounting {exec|commands]
Mode	Line Configuration

show accounting

Use this command to display ordered methods for accounting lists.

Format	show accounting
Mode	Privileged EXEC

The following shows example CLI display output for the command.

```
(CN1610) #show accounting
```

```
Number of Accounting Notifications sent at beginning of an EXEC
session:     0
Errors when sending Accounting Notifications beginning of an EXEC
session:          0
Number of Accounting Notifications at end of an EXEC session:
       0
Errors when sending Accounting Notifications at end of an EXEC
session:             0
Number of Accounting Notifications sent at beginning of a command
execution:        0
Errors when sending Accounting Notifications at beginning of a
command execution:   0
Number of Accounting Notifications sent at end of a command
execution:              0
Errors when sending Accounting Notifications at end of a command
execution:         0
```

show accounting methods

Use this command to display configured accounting method lists.

Format	`show accounting methods`
Mode	Privileged EXEC

The following shows example CLI display output for the command.

```
(CN1610) #
(CN1610) #show accounting methods

Acct Type    Method Name     Record Type    Method Type
----------   ------------    ------------   ------------
Exec   dfltExecList    start-stop TACACS
Commands     dfltCmdsList    stop-only TACACS
Commands UserCmdAudit start-stopTACACS
DOT1X dfltDot1xList start-stopradius

Line     EXEC Method List    Command Method List
-------  ----------------------------------------
Console  dfltExecList          dfltCmdsList
Telnet   dfltExecList          dfltCmdsList
SSH      dfltExecList          UserCmdAudit
```

clear accounting statistics

This command clears the accounting statistics.

Format	`clear accounting statistics`
Mode	Privileged EXEC

show domain-name This command displays the configured domain-name.

Format	`show domain-name`
Mode	Privileged EXEC

The following shows example CLI display output for the command.

```
(CN1610) #
(CN1610) #show domain-name

Domain                : Enable
Domain-name           :abc
```

SNMP Commands

This section describes the commands you use to configure Simple Network Management Protocol (SNMP) on the switch. You can configure the switch to act as an SNMP agent so that it can communicate with SNMP managers on your network.

snmp-server

This command sets the name and the physical location of the switch, and the organization responsible for the network. The parameters `name`, `loc` and `con` can be up to 255 characters in length.

Default	none
Format	`snmp-server {sysname` *`name`* `| location` *`loc`* `| contact` *`con`*`}`
Mode	Global Config

Note

To clear the snmp-server, enter an empty string in quotes. For example, snmp-server {sysname " "} clears the system name.

snmp-server community

This command adds (and names) a new SNMP community, and optionally sets the access mode, allowed IP address, and create a view for the community.

Note

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

Default	Two communities are created by default: ◆ public, with read-only permissions, a view name of Default, and allows access from all IP addresses ◆ private, with read/write permissions, a view name of Default, and allows access from all IP addresses.
Format	`snmp-server community` *`community-string`* `[{ro | rw |su }] [ipaddress` *`ip-address`*`]` *`[view view-name]`*

Mode	Global Config

Parameter	Description
community-name	A name associated with the switch and with a set of SNMP managers that manage it with a specified privileged level. The length of `community-name` can be up to 16 case-sensitive characters.
ro | rw | su	The access mode of the SNMP community, which can be public (Read-Only/RO), private (Read-Write/RW), or Super User (SU).
ip-address	The associated community SNMP packet sending address and is used along with the client IP mask value to denote a range of IP addresses from which SNMP clients may use that community to access the device. A value of 0.0.0.0 allows access from any IP address. Otherwise, this value is ANDed with the mask to determine the range of allowed client IP addresses.
view-name	The name of the view to create or update.

no snmp-server community

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

Format	`no snmp-server community` *`community-name`*
Mode	Global Config

snmp-server community-group

This command configures a community access string to permit access via the SNMPv1 and SNMPv2c protocols.

Format	`snmp-server community-group` *`community-string group-name`* `[ipaddress` *`ipaddress`*`]`
Mode	Global Config

Parameter	Description
community-string	The community which is created and then associated with the group. The range is 1 to 20 characters.
group-name	The name of the group that the community is associated with. The range is 1 to 30 characters.
ipaddress	Optionally, the IPv4 address that the community may be accessed from.

snmp-server enable traps violation

The Port MAC locking component interprets this command and configures violation action to send an SNMP trap with default trap frequency of 30 seconds. The Global command configures the trap violation mode across all interfaces valid for port-security. There is no global trap mode as such.

Note

For other port security commands, see "Port Security Commands" on page 540.

Default	disabled
Format	`snmp-server enable traps violation`
Mode	◆ Global Config ◆ Interface Config

no snmp-server enable traps violation

This command disables the sending of new violation traps.

Format	`no snmp-server enable traps violation`
Mode	Interface Config

snmp-server enable traps

This command enables the Authentication Flag.

Default	enabled
Format	`snmp-server enable traps`

Mode	Global Config

no snmp-server enable traps

This command disables the Authentication Flag.

Format	`no snmp-server enable traps`
Mode	Global Config

snmp trap link-status

This command enables link status traps on an interface or range of interfaces.

Note

This command is valid only when the Link Up/Down Flag is enabled. See "snmp trap link-status" on page 92

Format	`snmp trap link-status`
Mode	Interface Config

no snmp trap link-status

This command disables link status traps by interface.

Note

This command is valid only when the Link Up/Down Flag is enabled.

Format	`no snmp trap link-status`
Mode	Interface Config

snmp trap link-status all

This command enables link status traps for all interfaces.

Note

This command is valid only when the Link Up/Down Flag is enabled. See "snmp trap link-status" on page 92.

Format	`snmp trap link-status all`
Mode	Global Config

no snmp trap link-status all

This command disables link status traps for all interfaces.

Note

This command is valid only when the Link Up/Down Flag is enabled. See "snmp trap link-status" on page 92.

Format	`no snmp trap link-status all`
Mode	Global Config

snmp-server enable traps linkmode

This command enables Link Up/Down traps for the entire switch. When enabled, link traps are sent only if the Link Trap flag setting associated with the port is enabled. See "snmp trap link-status" on page 92.

Default	enabled
Format	`snmp-server enable traps linkmode`
Mode	Global Config

no snmp-server enable traps linkmode

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

Format	`no snmp-server enable traps linkmode`
Mode	Global Config

snmp-server enable traps multiusers

This command enables Multiple User traps. When the traps are enabled, a Multiple User Trap is sent when a user logs in to the terminal interface (EIA 232 or Telnet) and there is an existing terminal interface session.

Default	enabled
Format	`snmp-server enable traps multiusers`
Mode	Global Config

no snmp-server enable traps multiusers

This command disables Multiple User traps.

Format	`no snmp-server enable traps multiusers`
Mode	Global Config

snmp-server enable traps stpmode

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

Default	enabled
Format	`snmp-server enable traps stpmode`
Mode	Global Config

no snmp-server enable traps stpmode

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

Format	`no snmp-server enable traps stpmode`
Mode	Global Config

snmp-server engineID local

This command configures the SNMP engine ID on the local device.

Default	The engineID is configured automatically, based on the device MAC address.
Format	`snmp-server engineID local {`*`engineid-string`*`|default}`
Mode	Global Config

Parameter	Description
engineid-string	A hexadecimal string identifying the engine-id, used for localizing configuration. Engine-id must be an even length in the range of 6 to 32 hexadecimal characters.

Parameter	Description
default	Sets the engine-id to the default string, based on the device MAC address.

CAUTION

Changing the engine-id will invalidate all SNMP configuration that exists on the box.

no snmp-server engineID local

This command removes the specified engine ID.

Default	The engineID is configured automatically, based on the device MAC address.
Format	`no snmp-server engineID local`
Mode	Global Config

snmp-server filter

This command creates a filter entry for use in limiting which traps will be sent to a host.

Default	No filters are created by default.
Format	`snmp-server filter` *`filtername oid-tree`* `{included|excluded}`
Mode	Global Config

Parameter	Description
filtername	The label for the filter being created. The range is 1 to 30 characters.
oid-tree	The OID subtree to include or exclude from the filter. Subtrees may be specified by numerical (1.3.6.2.4) or keywords (system), and asterisks may be used to specify a subtree family (1.3.*.4).

Parameter	Description
included	The tree is included in the filter.
excluded	The tree is excluded from the filter.

no snmp-server filter

This command removes the specified filter.

Default	No filters are created by default.
Format	`snmp-server filter` *`filtername`* [*`oid-tree`*]
Mode	Global Config

snmp-server group

This command creates an SNMP access group.

Default	Generic groups are created for all versions and privileges using the default views.
Format	`snmp-server group` *`group-name`* {`v1` | `v2c` | `v3` {`noauth` | `auth` | `priv`}} [`context` *`context-name`*] [`read` *`read-view`*] [`write` *`write-view`*] [`notify` *`notify-view`*]
Mode	Global Config

Parameter	Description
group-name	The group name to be used when configuring communities or users. The range is 1 to 30 characters.
v1	This group can only access via SNMPv1.
v2	This group can only access via SNMPv2c.
v3	This group can only access via SNMPv3.
noauth	This group can be accessed only when not using Authentication or Encryption. Applicable only if SNMPv3 is selected.

Parameter	Description
auth	This group can be accessed only when using Authentication but not Encryption. Applicable only if SNMPv3 is selected.
priv	This group can be accessed only when using both Authentication and Encryption. Applicable only if SNMPv3 is selected.
context-name	The SNMPv3 context used during access. Applicable only if SNMPv3 is selected.
read-view	The view this group will use during GET requests. The range is 1 to 30 characters.
write-view	The view this group will use during SET requests. The range is 1 to 30 characters.
notify-view	The view this group will use when sending out traps. The range is 1 to 30 characters.

no snmp-server group

This command removes the specified group.

Format	`no snmp-server group` *`group-name`* `{v1|v2c| 3 {noauth|auth|priv}} [context context-name]`
Mode	Global Config

snmp-server host

This command configures traps to be sent to the specified host.

Default	No default hosts are configured.
Format	`snmp-server host` *`host-addr`* `{informs [timeout` *`seconds`*`] [retries` *`retries`*`]|traps version {1 | 2c }} community-string [udp-port` *`port`*`] [filter` *`filter-name`*`]`
Mode	Global Config

Parameter	Description
host-addr	The IPv4 or IPv6 address of the host to send the trap or inform to.
traps	Send SNMP traps to the host. This option is selected by default.
version 1	Sends SNMPv1 traps. This option is not available if informs is selected.
version 2	Sends SNMPv2c traps. This option is not available if informs is selected. This option is selected by default.
informs	Send SNMPv2 informs to the host.
seconds	The number of seconds to wait for an acknowledgement before resending the Inform. The default is 15 seconds. The range is 1 to 300 seconds.
retries	The number of times to resend an Inform. The default is 3 attempts. The range is 0 to 255 retries.
community-string	Community string sent as part of the notification. The range is 1 to 20 characters.
port	The SNMP Trap receiver port. The default is port 162.
filter-name	The filter name to associate with this host. Filters can be used to specify which traps are sent to this host. The range is 1 to 30 characters.

no snmp-server host

This command removes the specified host entry.

Format	`no snmp-server host` *`host-addr`* `[traps|informs]`
Mode	Global Config

snmp-server user

This command creates an SNMPv3 user for access to the system.

Default	No default users are created.
Format	`snmp-server user` *`username groupname`* `[remote` *`engineid-string`*`] [ {auth-md5` *`password`* `| auth-sha` *`password`* `| auth-md5-key` *`md5-key`* `| auth-sha-key` *`sha-key`*`} [priv-des` *`password`* `| priv-des-key` *`des-key`*`]`
Mode	Global Config

Parameter	**Description**
username	The username the SNMPv3 user will connect to the switch as. The range is 1 to 30 characters.
group-name	The name of the group the user belongs to. The range is 1 to 30 characters.
engineid-string	The engine-id of the remote management station that this user will be connecting from. The range is 5 to 32 characters.
password	The password the user will use for the authentication or encryption mechanism. The range is 1 to 32 characters.
md5-key	A pregenerated MD5 authentication key. The length is 32 characters.
sha-key	A pregenerated SHA authentication key. The length is 48 characters.
des-key	A pregenerated DES encryption key. The length is 32 characters if MD5 is selected, 48 characters if SHA is selected.

no snmp-server user

This command removes the specified SNMPv3 user.

Format	`no snmp-server user` *`username`*
Mode	Global Config

snmp-server view

This command creates or modifies an existing view entry that is used by groups to determine which objects can be accessed by a community or user.

Default	Views are created by default to provide access to the default groups.
Format	`snmp-server` *`viewname oid-tree`* `{included|excluded}`
Mode	Global Config

Parameter	Description
viewname	The label for the view being created. The range is 1 to 30 characters.
oid-tree	The OID subtree to include or exclude from the view. Subtrees may be specified by numerical (1.3.6.2.4) or keywords (system), and asterisks may be used to specify a subtree family (1.3.*.4).
included	The tree is included in the view.
excluded	The tree is excluded from the view.

no snmp-server view

This command removes the specified view.

Format	`no snmp-server view` *`viewname`* `[`*`oid-tree`*`]`
Mode	Global Config

snmp-server v3-host

This command configures traps to be sent to the specified host.

Default	No default hosts are configured.
Format	`snmp-server v3-host` *`host-addr username`* `[traps | informs [timeout` *`seconds`*`] [retries retries]] [auth | noauth | priv] [udpport` *`port`*`] [filter` *`filtername`*`]`
Mode	Global Config

Parameter	Description
host-addr	The IPv4 or IPv6 address of the host to send the trap or inform to.
user-name	User used to send a Trap or Inform message. This user must be associated with a group that supports the version and access method. The range is 1 to 30 characters.
traps	Send SNMP traps to the host. This is the default option.
informs	Send SNMP informs to the host.
seconds	Number of seconds to wait for an acknowledgement before resending the Inform. The default is 15 seconds. The range is 1 to 300 seconds.
retries	Number of times to resend an Inform. The default is 3 attempts. The range is 0 to 255 retries.
auth	Enables authentication but not encryption.
noauth	No authentication or encryption. This is the default.
priv	Enables authentication and encryption.
port	The SNMP Trap receiver port. This value defaults to port 162.
filter-name	The filter name to associate with this host. Filters can be used to specify which traps are sent to this host. The range is 1 to 30 characters.

show snmp

This command displays the current SNMP configuration.

Format	`show snmp`
Mode	Privileged EXEC

Term		Definition
Community Table:	Community-String	The community string for the entry. This is used by SNMPv1 and SNMPv2 protocols to access the switch.
	Community-Access	The type of access the community has: ◆ Read only ◆ Read write ◆ su
	View Name	The view this community has access to.
	IP Address	Access to this community is limited to this IP address.
Community Group Table:	Community-String	The community this mapping configures
	Group Name	The group this community is assigned to.
	IP Address	The IP address this community is limited to.

Term		Definition
Host Table:	Target Address	The address of the host that traps will be sent to.
	Type	The type of message that will be sent, either traps or informs.
	Community	The community traps will be sent to.
	Version	The version of SNMP the trap will be sent as.
	UDP Port	The UDP port the trap or inform will be sent to.
	Filter name	The filter the traps will be limited by for this host.
	TO Sec	The number of seconds before informs will time out when sending to this host.
	Retries	The number of times informs will be sent after timing out.

show snmp engineID

This command displays the currently configured SNMP engineID.

Format	`show snmp engineID`
Mode	Privileged EXEC

Parameter	Description
Local SNMP EnginID	The current configuration of the displayed SNMP engineID.

show snmp filters

This command displays the configured filters used when sending traps.

Format	`show snmp filters [filtername]`
Mode	Privileged EXEC

Parameter	Description
Name	The filter name for this entry.
OID Tree	The OID tree this entry will include or exclude.
Type	Indicates if this entry includes or excludes the OID Tree.

show snmp group

This command displays the configured groups.

Format	`show snmp group [groupname]`
Mode	Privileged EXEC

Parameter	Description
Name	The name of the group.
Security Model	Indicates which protocol can access the system via this group.
Security Level	Indicates the security level allowed for this group.
Read View	The view this group provides read access to.
Write View	The view this group provides write access to.
Notify View	The view this group provides trap access to.

show snmp source-interface

Use this command in Privileged EXEC mode to display the configured global source-interface (Source IP address) details used for an SNMP client.

Format	`show snmp source-interface`

Mode	Privileged EXEC

The following shows example CLI display output for the command.

```
(CN1610)# show snmp source-interface
SNMP trap Client Source Interface.............. (not configured)
```

show snmp user

This command displays the currently configured SNMPv3 users.

Format	`show snmp user [`*`username`*`]`
Mode	Privileged EXEC

Term	Definition
Name	The name of the user.
Group Name	The group that defines the SNMPv3 access parameters.
Auth Method	The authentication algorithm configured for this user.
Privilege Method	The encryption algorithm configured for this user.
Remote Engine ID	The engineID for the user defined on the client machine.

show snmp views

This command displays the currently configured views.

Format	`show snmp views [`*`viewname`*`]`
Mode	Privileged EXEC

Parameter	Description
Name	The view name for this entry.

Parameter	Description
OID Tree	The OID tree that this entry will include or exclude.
Type	Indicates if this entry includes or excludes the OID tree.

show trapflags

This command displays trap conditions. The command's display shows all the enabled OSPFv2 and OSPFv3 trapflags. Configure which traps the switch should generate by enabling or disabling the trap condition. If a trap condition is enabled and the condition is detected, the SNMP agent on the switch sends the trap to all enabled trap receivers. You do not have to reset the switch to implement the changes. Cold and warm start traps are always generated and cannot be disabled.

Format	`show trapflags`
Mode	Privileged EXEC

Term	Definition
Authentication Flag	Can be enabled or disabled. The factory default is enabled. Indicates whether authentication failure traps will be sent.
Link Up/Down Flag	Can be enabled or disabled. The factory default is enabled. Indicates whether link status traps will be sent.
Multiple Users Flag	Can be enabled or disabled. The factory default is enabled. Indicates whether a trap will be sent when the same user ID is logged into the switch more than once at the same time (either through Telnet or the serial port).
Spanning Tree Flag	Can be enabled or disabled. The factory default is enabled. Indicates whether spanning tree traps are sent.
ACL Traps	May be enabled or disabled. The factory default is disabled. Indicates whether ACL traps are sent.

RADIUS Commands

This section describes the commands you use to configure the switch to use a Remote Authentication Dial-In User Service (RADIUS) server on your network for authentication and accounting.

authorization network radius

Use this command to enable the switch to accept VLAN assignment by the radius server.

Default	disable
Format	`authorization network radius`
Mode	Global Config

no authorization network radius

Use this command to disable the switch to accept VLAN assignment by the radius server.

Format	`no authorization network radius`
Mode	Global Config

radius accounting mode

This command is used to enable the RADIUS accounting function.

Default	disabled
Format	`radius accounting mode`
Mode	Global Config

no radius accounting mode

This command is used to set the RADIUS accounting function to the default value - i.e. the RADIUS accounting function is disabled.

Format	`no radius accounting mode`
Mode	Global Config

radius server attribute 4

This command specifies the RADIUS client to use the NAS-IP Address attribute in the RADIUS requests. If the specific IP address is configured while enabling this attribute, the RADIUS client uses that IP address while sending NAS-IP-Address attribute in RADIUS communication.

Format	`radius server attribute 4 [`*`ipaddr`*`]`
Mode	Global Config

Term	Definition
4	NAS-IP-Address attribute to be used in RADIUS requests.
ipaddr	The IP address of the server.

no radius server attribute 4

The `no` version of this command disables the NAS-IP-Address attribute global parameter for RADIUS client. When this parameter is disabled, the RADIUS client does not send the NAS-IP-Address attribute in RADIUS requests.

Format	`no radius server attribute 4 [`*`ipaddr`*`]`
Mode	Global Config

The following shows an example of the command.

```
(CN1610) (Config) #radius server attribute 4  192.168.37.60
(CN1610) (Config) #radius server attribute 4
```

radius server host

This command configures the IP address or DNS name to use for communicating with the RADIUS server of a selected server type. While configuring the IP address or DNS name for the authenticating or accounting servers, you can also configure the port number and server name. If the authenticating and accounting servers are configured without a name, the command uses the Default_RADIUS_Auth_Server and Default_RADIUS_Acct_Server as the default names, respectively. The same name can be configured for more than one authenticating servers and the name should be unique for accounting servers. The RADIUS client allows the configuration of a maximum 32 authenticating and accounting servers.

If you use the *auth* parameter, the command configures the IP address or hostname to use to connect to a RADIUS authentication server. You can configure up to 3 servers per RADIUS client. If the maximum number of configured servers is reached, the command fails until you remove one of the servers by issuing the "no" form of the command. If you use the optional *port* parameter, the command configures the UDP port number to use when connecting to the configured RADIUS server. The *port* number range is 1 - 65535, with 1812 being the default value.

Note
To reconfigure a RADIUS authentication server to use the default UDP *port*, set the *port* parameter to 1812.

Note
If you use the *acct* token, the command configures the IP address or hostname to use for the RADIUS accounting server. You can only configure one accounting server. If an accounting server is currently configured, use the "no" form of the command to remove it from the configuration. The IP address or hostname you specify must match that of a previously configured accounting server. If you use the optional *port* parameter, the command configures the UDP port to use when connecting to the RADIUS accounting server. If a *port* is already configured for the accounting server, the new *port* replaces the previously configured *port*. The *port* must be a value in the range 0 - 65535, with 1813 being the default.

Note
To reconfigure a RADIUS accounting server to use the default UDP *port*, set the *port* parameter to 1813.

Format	`radius server host {auth | acct} {`*ipaddr*`|`*dnsname*`} [name` *servername*`] [port` *0-65535*`]`
Mode	Global Config

Field	Description
ipaddr	The IP address of the server.
dnsname	The DNS name of the server.
0-65535	The port number to use to connect to the specified RADIUS server.

Field	Description
servername	The alias name to identify the server.

no radius server host

The no version of this command deletes the configured server entry from the list of configured RADIUS servers. If the RADIUS authenticating server being removed is the active server in the servers that are identified by the same server name, then the RADIUS client selects another server for making RADIUS transactions. If the 'auth' token is used, the previously configured RADIUS authentication server is removed from the configuration. Similarly, if the 'acct' token is used, the previously configured RADIUS accounting server is removed from the configuration. The *ipaddr|dnsname* parameter must match the IP address or DNS name of the previously configured RADIUS authentication / accounting server.

Format	no radius server host {auth | acct} {*ipaddr|dnsname*}
Mode	Global Config

The following shows an example of the command.

```
(CN1610) (Config) #radius server host acct 192.168.37.60
(CN1610) (Config) #radius server host acct 192.168.37.60 port 1813
(CN1610) (Config) #radius server host auth 192.168.37.60 name
Network1_RS port 1813
(CN1610) (Config) #radius server host acct 192.168.37.60 name
Network2_RS
(CN1610) (Config) #no radius server host acct 192.168.37.60
```

radius server key

This command configures the key to be used in RADIUS client communication with the specified server. Depending on whether the 'auth' or 'acct' token is used, the shared secret is configured for the RADIUS authentication or RADIUS accounting server. The IP address or hostname provided must match a previously configured server. When this command is executed, the secret is prompted.

Text-based configuration supports Radius server's secrets in encrypted and non-encrypted format. When you save the configuration, these secret keys are stored in encrypted format only. If you want to enter the key in encrypted format, enter the key along with the encrypted keyword. In the "show running-config" on page 177 command's display, these secret keys are displayed in encrypted format. You cannot show these keys in plain text format.

Note

The secret must be an alphanumeric value not exceeding 16 characters.

Format	`radius server key {auth | acct} {`*`ipaddr`*`|`*`dnsname`*`} `*`encrypted password`*
Mode	Global Config

Field	Description
ipaddr	The IP address of the server.
dnsname	The DNS name of the server.
password	The password in encrypted format.

The following shows an example of the CLI command.
`radius server key acct 10.240.4.10 encrypted` *`encrypt-string`*

radius server msgauth

This command enables the message authenticator attribute to be used for the specified RADIUS Authenticating server.

Format	`radius server msgauth` *`ipaddr`*`|`*`dnsname`*
Mode	Global Config

Field	Description
ip addr	The IP address of the server.
dnsname	The DNS name of the server.

no radius server msgauth

The `no` version of this command disables the message authenticator attribute to be used for the specified RADIUS Authenticating server.

Format	`no radius server msgauth` *`ipaddr`*`|`*`dnsname`*
Mode	Global Config

radius server primary

This command specifies a configured server that should be the primary server in the group of servers which have the same server name. Multiple primary servers can be configured for each number of servers that have the same name. When the RADIUS client has to perform transactions with an authenticating RADIUS server of specified name, the client uses the primary server that has the specified server name by default. If the RADIUS client fails to communicate with the primary server for any reason, the client uses the backup servers configured with the same server name. These backup servers are identified as the Secondary type.

Format	`radius server primary {`*`ipaddr`*`|`*`dnsname`*`}`
Mode	Global Config

Field	Description
ip addr	The IP address of the RADIUS Authenticating server.
dnsname	The DNS name of the server.

radius server retransmit

This command configures the global parameter for the RADIUS client that specifies the number of transmissions of the messages to be made before attempting the fall back server upon unsuccessful communication with the current RADIUS authenticating server. When the maximum number of retries are exhausted for the RADIUS accounting server and no response is received, the client does not communicate with any other server.

Default	4
Format	`radius server retransmit` *`retries`*
Mode	Global Config

Field	Description
retries	The maximum number of transmission attempts in the range of 1 to 15.

no radius server retransmit

The no version of this command sets the value of this global parameter to the default value.

Format	`no radius server retransmit`
Mode	Global Config

radius server timeout

This command configures the global parameter for the RADIUS client that specifies the timeout value (in seconds) after which a request must be retransmitted to the RADIUS server if no response is received. The timeout value is an integer in the range of 1 to 30.

Default	5
Format	`radius server timeout` *`seconds`*
Mode	Global Config

Field	Description
retries	Maximum number of transmission attempts in the range 1–30.

no radius server timeout

The no version of this command sets the timeout global parameter to the default value.

Format	`no radius server timeout`
Mode	Global Config

show radius servers

Use this command to display the authentication parameters.

Default	Not applicable
Format	`show radius servers { `*`serverIP`*` | name `*`serverName`*` }`
Mode	User EXEC

```
(CN1610)# show radius servers name Default-RADIUS-Server

RADIUS Server Name.............................. CoA-Server-1
Current Server IP Address....................... 1.1.1.1
Number of Retransmits........................... 3
Timeout Duration................................ 15
Deadtime........................................ 0
Port............................................ 3799
Source IP....................................... 10.27.9.99 <-
switch
RADIUS Accounting Mode.......................... Disabled
Secret Configured............................... Yes
Message Authenticator........................... Enable
Number of CoA Requests Received..................... 203
Number of CoA ACK Responses Sent.................... 111
Number of CoA NAK Responses Sent..................... 37
Number of Coa Requests Ignored....................... 55
Number of CoA Missing/Unsupported Attribute Requests.....  18
Number of CoA Session Context Not Found Requests.........  5
Number of CoA Invalid Attribute Value Requests... 11
Number of Administratively Prohibited Requests.........3
```

show radius

This command displays the values configured for the global parameters of the RADIUS client.

Format	`show radius`
Mode	Privileged EXEC

Output	Description
`Number of Configured Authentication Servers`	The number of RADIUS Authentication servers that have been configured.
`Number of Configured Accounting Servers`	The number of RADIUS Accounting servers that have been configured.

Output	Description
Number of Named Authentication Server Groups	The number of configured named RADIUS server groups.
Number of Named Accounting Server Groups	The number of configured named RADIUS server groups.
Number of Retransmits	The configured value of the maximum number of times a request packet is retransmitted.
Time Duration	The configured timeout value, in seconds, for request retransmissions.
RADIUS Accounting Mode	A global parameter to indicate whether or not the accounting mode for all the servers is enabled.
RADIUS Attribute 4 Mode	A global parameter to indicate whether the NAS-IP-Address attribute has been enabled for use in RADIUS requests.
RADIUS Attribute 4 Value	A global parameter that specifies the IP address to be used in the NAS-IP-Address attribute of RADIUS requests.

The following shows example CLI display output for the command.

```
(CN1610) #show radius

        Number of Configured Authentication Servers..... 32
        Number of Configured Accounting Servers......... 32
        Number of Named Authentication Server Groups..... 15
        Number of Named Accounting Server Groups........ 3
        Number of Retransmits........................... 4
        Time Duration................................... 10
        RADIUS Accounting Mode..................... Disable
        RADIUS Attribute 4 Mode..................... Enable
       RADIUS Attribute 4 Value ..... 192.168.37.60
```

show radius servers

This command displays the summary and details of RADIUS authenticating servers configured for the RADIUS client.

Format	`show radius servers [{`*`ipaddr`*`/`*`dnsname`*` | name [servername]}]`
Mode	Privileged EXEC

Field	Description
ipaddr	The IP address of the authenticating server.
dnsname	The DNS name of the authenticating server.
servername	The alias name to identify the server.
Current	The * symbol preceding the server host address specifies that the server is currently active.
Host Address	The IP address of the host.
Server Name	The name of the authenticating server.
Port	The port used for communication with the authenticating server.
Type	Specifies whether this server is a primary or secondary type.
Current Host Address	The IP address of the currently active authenticating server.
Secret Configured	Yes or No Boolean value that indicates whether this server is configured with a secret.
Number of Retransmits	The configured value of the maximum number of times a request packet is retransmitted.
Message Authenticator	A global parameter to indicate whether the Message Authenticator attribute is enabled or disabled.
Time Duration	The configured timeout value, in seconds, for request retransmissions.
RADIUS Accounting Mode	A global parameter to indicate whether the accounting mode for all the servers is enabled or not.

Field	Description
RADIUS Attribute 4 Mode	A global parameter to indicate whether the NAS-IP-Address attribute has been enabled to use in RADIUS requests.
RADIUS Attribute 4 Value	A global parameter that specifies the IP address to be used in NAS-IP-Address attribute used in RADIUS requests.

The following shows example CLI display output for the command.

```
(CN1610) #show radius servers

Cur  Host Address             Server Name                      Port
Type
rent
---- ----------------------- -------------------------------- ---
-- ----------
 *   192.168.37.200          Network1_RADIUS_Server           1813
Primary
     192.168.37.201          Network2_RADIUS_Server           1813
Secondary
     192.168.37.202          Network3_RADIUS_Server           1813
Primary
     192.168.37.203          Network4_RADIUS_Server           1813
Secondary

(CN1610) #show radius servers name

Current Host Address     Server Name                        Type
------------------------ -------------------------------- -------
---192.168.37.200           Network1_RADIUS_Server
Secondary
192.168.37.201           Network2_RADIUS_Server            Primary
192.168.37.202          Network3_RADIUS_Server           Secondary
192.168.37.203           Network4_RADIUS_Server            Primary

(CN1610) #show radius servers name Default_RADIUS_Server

Server Name.............................. Default_RADIUS_Server
Host Address............................. 192.168.37.58
Secret Configured....................... No
Message Authenticator ................... Enable
Number of Retransmits.................... 4
Time Duration............................ 10
```

```
RADIUS Accounting Mode.................. Disable
RADIUS Attribute 4 Mode................. Enable
RADIUS Attribute 4 Value ............... 192.168.37.60

(CN1610) #show radius servers 192.168.37.58

Server Name............................. Default_RADIUS_Server
Host Address............................ 192.168.37.58
Secret Configured....................... No
Message Authenticator .................. Enable
Number of Retransmits................... 4
Time Duration........................... 10
RADIUS Accounting Mode.................. Disable
RADIUS Attribute 4 Mode................. Enable
RADIUS Attribute 4 Value ............... 192.168.37.60
```

show radius accounting

This command displays a summary of configured RADIUS accounting servers.

Format	`show radius accounting name [`*`servername`*`]`
Mode	Privileged EXEC

Field	Description
servername	An alias name to identify the server.
RADIUS Accounting Mode	A global parameter to indicate whether the accounting mode for all the servers is enabled or not.

If you do not specify any parameters, then only the accounting mode and the RADIUS accounting server details are displayed.

Term	Definition
Host Address	The IP address of the host.
Server Name	The name of the accounting server.
Port	The port used for communication with the accounting server.

Term	Definition
Secret Configured	Yes or No Boolean value indicating whether this server is configured with a secret.

The following shows example CLI display output for the command.

```
(CN1610) #show radius accounting name

Host Address            Server Name                         Port
Secret

Configured
---------------------- ---------------------------------- --------
-----------
192.168.37.200          Network1_RADIUS_Server             1813
Yes
192.168.37.201         Network2_RADIUS_Server            1813     No
192.168.37.202          Network3_RADIUS_Server             1813
Yes
192.168.37.203         Network4_RADIUS_Server            1813     No


 (CN1610) #show radius accounting name Default_RADIUS_Server

Server Name..................................... Default_RADIUS_Server
Host Address.................................... 192.168.37.200
RADIUS Accounting Mode.......................... Disable
Port ........................................... 1813
Secret Configured .............................. Yes
```

show radius accounting statistics

This command displays a summary of statistics for the configured RADIUS accounting servers.

Format	`show radius accounting statistics {`*`ipaddr`*`|`*`dnsname`*`	name `*`servername`*`}`
Mode	Privileged EXEC

Term	Definition
ipaddr	The IP address of the server.

Term	Definition
dnsname	The DNS name of the server.
servername	The alias name to identify the server.
RADIUS Accounting Server Name	The name of the accounting server.
Server Host Address	The IP address of the host.
Round Trip Time	The time interval, in hundredths of a second, between the most recent Accounting-Response and the Accounting-Request that matched it from this RADIUS accounting server.
Requests	The number of RADIUS Accounting-Request packets sent to this server. This number does not include retransmissions.
Retransmission	The number of RADIUS Accounting-Request packets retransmitted to this RADIUS accounting server.
Responses	The number of RADIUS packets received on the accounting port from this server.
Malformed Responses	The number of malformed RADIUS Accounting-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators or signature attributes or unknown types are not included as malformed accounting responses.
Bad Authenticators	The number of RADIUS Accounting-Response packets containing invalid authenticators received from this accounting server.
Pending Requests	The number of RADIUS Accounting-Request packets sent to this server that have not yet timed out or received a response.
Timeouts	The number of accounting timeouts to this server.

Term	Definition
Unknown Types	The number of RADIUS packets of unknown types, which were received from this server on the accounting port.
Packets Dropped	The number of RADIUS packets received from this server on the accounting port and dropped for some other reason.

The following shows example CLI display output for the command.

```
(CN1610) #show radius accounting statistics 192.168.37.200

RADIUS Accounting Server Name.................
Default_RADIUS_Server
Host Address.................................. 192.168.37.200
Round Trip Time............................... 0.00
Requests...................................... 0
Retransmissions............................... 0
Responses..................................... 0
Malformed Responses........................... 0
Bad Authenticators............................ 0
Pending Requests.............................. 0
Timeouts...................................... 0
Unknown Types................................. 0
Packets Dropped............................... 0

(CN1610) #show radius accounting statistics name
Default_RADIUS_Server

RADIUS Accounting Server Name.................
Default_RADIUS_Server
Host Address.................................. 192.168.37.200
Round Trip Time............................... 0.00
Requests...................................... 0
Retransmissions............................... 0
Responses..................................... 0
Malformed Responses........................... 0
Bad Authenticators............................ 0
Pending Requests.............................. 0
Timeouts...................................... 0
Unknown Types................................. 0
Packets Dropped............................... 0
```

show radius statistics

This command displays the summary statistics of configured RADIUS Authenticating servers.

Format	`show radius statistics {`*`ipaddr`*`|`*`dnsname`* `| name` *`servername`*`}`
Mode	Privileged EXEC

Term	Definition
ipaddr	The IP address of the server.
dnsname	The DNS name of the server.
servername	The alias name to identify the server.
RADIUS Server Name	The name of the authenticating server.
Server Host Address	The IP address of the host.
Access Requests	The number of RADIUS Access-Request packets sent to this server. This number does not include retransmissions.
Access Retransmissions	The number of RADIUS Access-Request packets retransmitted to this RADIUS authentication server.
Access Accepts	The number of RADIUS Access-Accept packets, including both valid and invalid packets, that were received from this server.
Access Rejects	The number of RADIUS Access-Reject packets, including both valid and invalid packets, that were received from this server.
Access Challenges	The number of RADIUS Access-Challenge packets, including both valid and invalid packets, that were received from this server.

Term	Definition
Malformed Access Responses	The number of malformed RADIUS Access-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators or signature attributes or unknown types are not included as malformed access responses.
Bad Authenticators	The number of RADIUS Access-Response packets containing invalid authenticators or signature attributes received from this server.
Pending Requests	The number of RADIUS Access-Request packets destined for this server that have not yet timed out or received a response.
Timeouts	The number of authentication timeouts to this server.
Unknown Types	The number of packets of unknown type that were received from this server on the authentication port.
Packets Dropped	The number of RADIUS packets received from this server on the authentication port and dropped for some other reason.

The following shows example CLI display output for the command.

```
(CN1610) #show radius statistics 192.168.37.200

RADIUS Server Name.....................
Default_RADIUS_Server
Server Host Address..................... 192.168.37.200
Access Requests.......................... 0.00
Access Retransmissions................... 0
Access Accepts........................... 0
Access Rejects........................... 0
Access Challenges........................ 0
Malformed Access Responses............... 0
Bad Authenticators....................... 0
Pending Requests......................... 0
Timeouts................................. 0
Unknown Types............................ 0
Packets Dropped.......................... 0
```

```
(CN1610) #show radius statistics name Default_RADIUS_Server

RADIUS Server Name.....................
Default_RADIUS_Server
Server Host Address..................... 192.168.37.200
Access Requests.......................... 0.00
Access Retransmissions................... 0
Access Accepts........................... 0
Access Rejects........................... 0
Access Challenges........................ 0
Malformed Access Responses............... 0
Bad Authenticators....................... 0
Pending Requests......................... 0
Timeouts................................. 0
Unknown Types............................ 0
Packets Dropped.......................... 0
```

TACACS+ Commands

TACACS+ provides access control for networked devices via one or more centralized servers. Similar to RADIUS, this protocol simplifies authentication by making use of a single database that can be shared by many clients on a large network. TACACS+ is based on the TACACS protocol (described in RFC1492) but additionally provides for separate authentication, authorization, and accounting services. The original protocol was UDP based with messages passed in clear text over the network; TACACS+ uses TCP to ensure reliable delivery and a shared key configured on the client and daemon server to encrypt all messages.

tacacs-server host

Use the `tacacs-server host` command in Global Configuration mode to configure a TACACS+ server. This command enters into the TACACS+ configuration mode. The *`ip-address|hostname`* parameter is the IP address or hostname of the TACACS+ server. To specify multiple hosts, multiple `tacacs-server host` commands can be used.

Format	`tacacs-server host` *`ip-address|hostname`*
Mode	Global Config

no tacacs-server host

Use the `no tacacs-server host` command to delete the specified hostname or IP address. The *`ip-address|hostname`* parameter is the IP address of the TACACS+ server.

Format	`no tacacs-server host` *`ip-address|hostname`*
Mode	Global Config

tacacs-server key

Use the `tacacs-server key` command to set the authentication and encryption key for all TACACS+ communications between the switch and the TACACS+ daemon. The *`key-string`* parameter has a range of 0 - 128 characters and specifies the authentication and encryption key for all TACACS communications between the switch and the TACACS+ server. This key must match the key used on the TACACS+ daemon.

Text-based configuration supports TACACS server's secrets in encrypted and non-encrypted format. When you save the configuration, these secret keys are stored in encrypted format only. If you want to enter the key in encrypted format, enter the key along with the encrypted keyword. In the "show running-config" on page 177 command's display, these secret keys are displayed in encrypted format. You cannot show these keys in plain text format.

Format	`tacacs-server key [key-string | encrypted key-string]`
Mode	Global Config

no tacacs-server key

Use the `no tacacs-server key` command to disable the authentication and encryption key for all TACACS+ communications between the switch and the TACACS+ daemon. The *key-string* parameter has a range of 0 - 128 characters This key must match the key used on the TACACS+ daemon.

Format	`no tacacs-server key key-string`
Mode	Global Config

tacacs-server keystring

Use the `tacacs-server keystring` command to set the global authentication encryption key used for all TACACS+ communications between the TACACS+ server and the client.

Format	`tacacs-server keystring`
Mode	Global Config

The following shows an example of the CLI command.

```
(Switching)(Config)#tacacs-server keystring
Enter tacacs key:********
Re-enter tacacs key:********
```

tacacs-server timeout

Use the `tacacs-server timeout` command to set the timeout value for communication with the TACACS+ servers. The *timeout* parameter has a range of 1-30 and is the timeout value in seconds. If you do not specify a timeout value, the command sets the global timeout to the default value. TACACS+ servers that do not use the global timeout will retain their configured timeout values.

Default	5
Format	`tacacs-server timeout` *`timeout`*
Mode	Global Config

no tacacs-server timeout

Use the `no tacacs-server timeout` command to restore the default timeout value for all TACACS servers.

Format	`no tacacs-server timeout`
Mode	Global Config

key

Use the `key` command in TACACS Configuration mode to specify the authentication and encryption key for all TACACS communications between the device and the TACACS server. This key must match the key used on the TACACS daemon. The *`key-string`* parameter specifies the key name. For an empty string use " ". (Range: 0 - 128 characters).

Text-based configuration supports TACACS server's secrets in encrypted and non-encrypted format. When you save the configuration, these secret keys are stored in encrypted format only. If you want to enter the key in encrypted format, enter the key along with the encrypted keyword. In the "show running-config" on page 177 command's display, these secret keys are displayed in encrypted format. You cannot show these keys in plain text format.

Format	`key [`*`key-string`* `|` `encrypted` *`key-string`*`]`
Mode	TACACS Config

keystring

Use the `keystring` command in TACACS Server Configuration mode to set the TACACS+ server-specific authentication encryption key used for all TACACS+ communications between the TACACS+ server and the client.

Format	`keystring`
Mode	TACACS Server Config

The following shows an example of the command.

```
(Switching)(Config)#tacacs-server host 1.1.1.1
(Switching)(Tacacs)#keystring

Enter tacacs key:********
Re-enter tacacs key:********
```

port

Use the `port` command in TACACS Configuration mode to specify a server port number. The server *`port-number`* range is 0 - 65535.

Default	49
Format	`port` *`port-number`*
Mode	TACACS Config

priority (TACACS Config)

Use the `priority` command in TACACS Configuration mode to specify the order in which servers are used, where 0 (zero) is the highest priority. The *`priority`* parameter specifies the priority for servers. The highest priority is 0 (zero), and the range is 0 - 65535.

Default	0
Format	`priority` *`priority`*
Mode	TACACS Config

timeout

Use the `timeout` command in TACACS Configuration mode to specify the timeout value in seconds. If no timeout value is specified, the global value is used. The *`timeout`* parameter has a range of 1-30 and is the timeout value in seconds.

Format	`timeout` *`timeout`*
Mode	TACACS Config

show tacacs

Use the `show tacacs` command to display the configuration, statistics, and source interface details of the TACACS+ client.

Format	`show tacacs [ip-address|hostname|client|server]`
Mode	Privileged EXEC

Term	Definition
Host address	The IP address or hostname of the configured TACACS+ server.
Port	The configured TACACS+ server port number.
TimeOut	The timeout in seconds for establishing a TCP connection.
Priority	The preference order in which TACACS+ servers are contacted. If a server connection fails, the next highest priority server is contacted.

Configuration Scripting Commands

Configuration Scripting allows you to generate text-formatted script files representing the current configuration of a system. You can upload these configuration script files to a PC or UNIX system and edit them. Then, you can download the edited files to the system and apply the new configuration. You can apply configuration scripts to one or more switches with no or minor modifications.

Use the `show running-config` command (see "show running-config" on page 177) to capture the running configuration into a script. Use the `copy` command (see "copy" on page 219) to transfer the configuration script to or from the switch.

Use the `show` command to view the configuration stored in the startup-config, backup-config, or factory-defaults file (see "show" on page 180).

You should use scripts on systems with default configuration; however, you are not prevented from applying scripts on systems with non-default configurations.

Scripts must conform to the following rules:

- The file extension must be ".scr".
- A maximum of ten scripts are allowed on the switch.
- The combined size of all script files on the switch shall not exceed 2048 KB.
- The maximum number of configuration file command lines is 2000.

You can type single-line annotations at the command prompt to use when you write test or configuration scripts to improve script readability. The exclamation point (!) character flags the beginning of a comment. The comment flag character can begin a word anywhere on the command line, and all input following this character is ignored. Any command line that begins with the "!" character is recognized as a comment line and ignored by the parser.

The following lines show an example of a script:

```
! Script file for displaying management access

show telnet !Displays the information about remote connections

! Display information about direct connections

show serial

! End of the script file!
```

Note

To specify a blank password for a user in the configuration script, you must specify it as a space within quotes. For example, to change the password for user jane from a blank password to hello, the script entry is as follows:

```
users passwd jane
" "
hello
hello
```

script apply

This command applies the commands in the script to the switch. The *scriptname* parameter is the name of the script to apply.

Format	`script apply` *scriptname*
Mode	Privileged EXEC

script delete

This command deletes a specified script where the *scriptname* parameter is the name of the script to delete. The *all* option deletes all the scripts present on the switch.

Format	`script delete {`*scriptname* `| all}`
Mode	Privileged EXEC

script list

This command lists all scripts present on the switch as well as the remaining available space.

Format	`script list`
Mode	Privileged EXEC

Term	Definition
Configuration Script	Name of the script.
Size	Privileged EXEC

script show

This command displays the contents of a script file, which is named *scriptname*.

Format	`script show` *scriptname*
Mode	Privileged EXEC

Term	Definition
Output Format	`line` *number*`:` *line contents*

script validate

This command validates a script file by parsing each line in the script file where *scriptname* is the name of the script to validate.The validate option is intended to be used as a tool for script development. Validation identifies potential problems. It might not identify all problems with a given script on any given device.

Format	`script validate` *scriptname*
Mode	Privileged EXEC

Prelogin Banner, System Prompt, and Host Name Commands

This section describes the commands you use to configure the prelogin banner and the system prompt. The prelogin banner is the text that displays before you login at the `User:` prompt.

copy (pre-login banner)

The `copy` command includes the option to upload or download the CLI Banner to or from the switch. You can specify local URLs by using FTP, TFTP, SFTP, SCP, or Xmodem.

Note

The parameter *ip6address* is also a valid parameter for routing packages that support IPv6.

Default	none

Format	`copy <tftp://<ipaddr>/<filepath>/<filename>> nvram:clibanner`
	
	`copy nvram:clibanner <tftp://<ipaddr>/<filepath>/<filename>>`

Mode	Privileged EXEC

set prompt

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

Format	`set prompt` *`prompt_string`*
Mode	Privileged EXEC

hostname

This command sets the system hostname. It also changes the prompt. The length of name may be up to 64 alphanumeric, case-sensitive characters.

Format	`hostname` *`hostname`*
Mode	Privileged EXEC

show clibanner

Use this command to display the configured prelogin CLI banner. The prelogin banner is the text that displays before displaying the CLI prompt.

Default	No contents to display before displaying the login prompt.
Format	`show clibanner`
Mode	Privileged EXEC

The following shows example CLI display output for the command.

```
(CN1610) #show clibanner

Banner Message configured :
=========================


--------------------------
         TEST
--------------------------
```

set clibanner

Use this command to configure the prelogin CLI banner before displaying the login prompt.

Format	`set clibanner` *line*
Mode	Global Config

Parameter	Description
line	Banner text where “” (double quote) is a delimiting character. The banner message can be up to 2000 characters.

no set clibanner

Use this command to unconfigure the prelogin CLI banner.

Format	`no set clibanner`
Mode	Global Config

Utility Commands 4

This chapter describes the utility commands available in the FASTPATH CLI.

The Utility Commands chapter includes the following sections:

The commands in this chapter are in one of four functional groups:

- Show commands display switch settings, statistics, and other information.
- Configuration commands configure features and options of the switch. For every configuration command, there is a show command that displays the configuration setting.
- Copy commands transfer or save configuration and informational files to and from the switch.
- Clear commands clear some or all of the settings to factory defaults.

AutoInstall Commands

The AutoInstall feature enables the automatic update of the image and configuration of the switch. This feature enables touchless or low-touch provisioning to simplify switch configuration and imaging.

AutoInstall includes the following support:

- Downloading an image from TFTP server using DHCP option 125. The image update can result in a downgrade or upgrade of the firmware on the switch.
- Automatically downloading a configuration file from a TFTP server when the switch is booted with no saved configuration file.
- Automatically downloading an image from a TFTP server in the following situations:
  - When the switch is booted with no saved configuration found.
  - When the switch is booted with a saved configuration that has AutoInstall enabled.

When the switch boots and no configuration file is found, it attempts to obtain an IP address from a network DHCP server. The response from the DHCP server includes the IP address of the TFTP server where the image and configuration flies are located.

After acquiring an IP address and the additional relevant information from the DHCP server, the switch downloads the image file or configuration file from the TFTP server. A downloaded image is automatically installed. A downloaded configuration file is saved to non-volatile memory.

Note

AutoInstall from a TFTP server can run on any IP interface, including the network port, service port, and in-band routing interfaces (if supported). To support AutoInstall, the DHCP client is enabled operationally on the service port, if it exists, or the network port, if there is no service port.

boot autoinstall

Use this command to operationally start or stop the AutoInstall process on the switch. The command is non-persistent and is not saved in the startup or running configuration file.

Default	stopped

Format	`boot autoinstall {start | stop}`
Mode	Privileged EXEC

boot host retrycount

Use this command to set the number of attempts to download a configuration file from the TFTP server.

Default	3
Format	`boot host retrycount` *`1-3`*
Mode	Privileged EXEC

no boot host retrycount

Use this command to set the number of attempts to download a configuration file to the default value.

Format	`no boot host retrycount`
Mode	Privileged EXEC

boot host dhcp

Use this command to enable AutoInstall on the switch for the next reboot cycle. The command does not change the current behavior of AutoInstall and saves the command to NVRAM.

Default	enabled
Format	`boot host dhcp`
Mode	Privileged EXEC

no boot host dhcp

Use this command to disable AutoInstall for the next reboot cycle.

Format	`no boot host dhcp`
Mode	Privileged EXEC

boot host autosave

Use this command to automatically save the downloaded configuration file to the startup-config file on the switch. When autosave is disabled, you must explicitly save the downloaded configuration to non-volatile memory by using the `write memory` or `copy system:running-config nvram:startup-config` command. If the switch reboots and the downloaded configuration has not been saved, the AutoInstall process begins, if the feature is enabled.

Default	disabled
Format	`boot host autosave`
Mode	Privileged EXEC

no boot host autosave

Use this command to disable automatically saving the downloaded configuration on the switch.

Format	`no boot host autosave`
Mode	Privileged EXEC

boot host autoreboot

Use this command to allow the switch to automatically reboot after successfully downloading an image. When auto reboot is enabled, no administrative action is required to activate the image and reload the switch.

Default	enabled
Format	`boot host autoreboot`
Mode	Privileged EXEC

no boot host autoreboot

Use this command to prevent the switch from automatically rebooting after the image is downloaded by using the AutoInstall feature.

Format	`no boot host autoreboot`
Mode	Privileged EXEC

erase startup-config

Use this command to erase the text-based configuration file stored in non-volatile memory. If the switch boots and no startup-config file is found, the AutoInstall process automatically begins.

Format	`erase startup-config`
Mode	Privileged EXEC

erase factory-defaults

Use this command to erase the text-based factory-defaults file stored in non-volatile memory.

Default	Disable
Format	`erase factory-defaults`
Mode	Privileged EXEC

show autoinstall

This command displays the current status of the AutoInstall process.

Format	`show autoinstall`
Mode	Privileged EXEC

The following shows example CLI display output for the command.

```
(CN1610) #show autoinstall

AutoInstall Mode.............................. Stopped
AutoInstall Persistent Mode................... Disabled
AutoSave Mode................................. Disabled
AutoReboot Mode............................... Enabled
AutoInstall Retry Count....................... 3
```

CLI Output Filtering Commands

show *xxx*|include "*string*"

The command ***xxx*** is executed and the output is filtered to only show lines containing the "***string***" match. All other non-matching lines in the output are suppressed.

The following shows an example of the CLI command.

```
(CN1610) #show running-config | include "spanning-tree"

spanning-tree configuration name "00-02-BC-42-F9-33"
spanning-tree bpduguard
spanning-tree bpdufilter default
spanning-tree forceversion 802.1w
```

show *xxx*|include "*string*" exclude "*string2*"

The command ***xxx*** is executed and the output is filtered to only show lines containing the "***string***" match and not containing the "***string2***" match. All other non-matching lines in the output are suppressed. If a line of output contains both the include and exclude strings then the line is not displayed.

The following shows example of the CLI command.

```
(CN1610) #show running-config | include "spanning-tree" exclude
"configuration"

spanning-tree bpduguard
spanning-tree bpdufilter default
spanning-tree forceversion 802.1w
```

show *xxx*|exclude "*string*"

The command ***xxx*** is executed and the output is filtered to show all lines not containing the "***string***" match. Output lines containing the "***string***" match are suppressed.

The following shows an example of the CLI command.

```
(CN1610) #show interface 0/1

Packets Received Without Error..... 0
Packets Received With Error..... 0
Broadcast Packets Received..... 0
Receive Packets Discarded..... 0
Packets Transmitted Without Errors..... 0
Transmit Packets Discarded..... 0
```

```
Transmit Packet Errors..... 0
Collision Frames..... 0
Number of link down events..... 1
Time Since Counters Last Cleared..... 281 day 4 hr 9 min
0 sec

(CN1610) #show interface 0/1 | exclude "Packets"

Transmit Packet Errors..... 0
Collision Frames..... 0
Number of link down events..... 1
Time Since Counters Last Cleared..... 20 day 21 hr 30 min
9 sec
```

show *xxx*|begin "*string*"

The command ***xxx*** is executed and the output is filtered to show all lines beginning with and following the first line containing the "***string***" match. All prior lines are suppressed.

The following shows an example of the CLI command.

```
(CN1610) #show port all | begin "1/1"

1/1          Enable                         Down   Disable N/A    N/A
1/2          Enable                         Down   Disable N/A    N/A
1/3          Enable                         Down   Disable N/A    N/A
1/4          Enable                         Down   Disable N/A    N/A
1/5          Enable                         Down   Disable N/A    N/A
1/6          Enable                         Down   Disable N/A    N/A

(CN1610) #
```

show *xxx*|section "*string*"

The command ***xxx*** is executed and the output is filtered to show only lines included within the section(s) identified by lines containing the "***string***" match and ending with the first line containing the default end-of-section identifier (i.e. "exit").

The following shows an example of the CLI command.

```
(CN1610) #show running-config | section "interface 0/1"

interface 0/1
no spanning-tree port mode
exit
```

show *xxx*|section "*string*" "*string2*"

The command ***xxx*** is executed and the output is filtered to only show lines included within the section(s) identified by lines containing the "***string***" match and ending with the first line containing the "***string2***" match. If multiple sessions matching the specified string match criteria are part of the base output, then all instances are displayed.

show *xxx*|section "*string*" include "*string2*"

The command ***xxx*** is executed and the output is filtered to only show lines included within the section(s) identified by lines containing the "***string***" match and ending with the first line containing the default end-of-section identifier (i.e. "exit") and that include the "string2" match. This type of filter command could also include "exclude" or user-defined end-of-section identifier parameters as well.

Dual Image Commands

FASTPATH software supports a dual image feature that allows the switch to have two software images in the permanent storage. You can specify which image is the active image to be loaded in subsequent reboots. This feature allows reduced down-time when you upgrade or downgrade the software.

delete

This command deletes the backup image file from the permanent storage or the core dump file from the local file system.

Format	`delete backup` `delete core-dump-file` *`file-name`* `| all`
Mode	Privileged EXEC

boot system

This command activates the specified image. It will be the active-image for subsequent reboots and will be loaded by the boot loader. The current active-image is marked as the backup-image for subsequent reboots. If the specified image doesn't exist on the system, this command returns an error message.

Format	`boot system {active | backup}`
Mode	Privileged EXEC

show bootvar

This command displays the version information and the activation status for the current active and backup images. The command also displays any text description associated with an image. This command displays the switch activation status.

Format	`show bootvar`
Mode	Privileged EXEC

filedescr

This command associates a given text description with an image. Any existing description will be replaced.

Format	`filedescr {active | backup}` *`text-description`*

Mode	Privileged EXEC

update bootcode

This command updates the bootcode (boot loader) on the switch. The bootcode is read from the active-image for subsequent reboots.

Format	`update bootcode`
Mode	Privileged EXEC

System Information and Statistics Commands

This section describes the commands you use to view information about system features, components, and configurations.

show arp switch

This command displays the contents of the IP stack's Address Resolution Protocol (ARP) table. The IP stack only learns ARP entries associated with the management interfaces - network or service ports. ARP entries associated with routing interfaces are not listed.

Format	`show arp switch`
Mode	Privileged EXEC

Term	Definition
IP Address	IP address of the management interface or another device on the management network.
MAC Address	Hardware MAC address of that device.
Interface	For a service port the output is *Management*. For a network port, the output is the slot/port of the physical interface.

show eventlog

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

Format	`show eventlog`
Mode	Privileged EXEC

Term	Definition
File	The file in which the event originated.
Line	The line number of the event.
Task Id	The task ID of the event.

Term	Definition
Code	The event code.
Time	The time this event occurred.

Note

Event log information is retained across a switch reset.

show version

This command displays inventory information for the switch.

Format	`show version`
Mode	Privileged EXEC

Term	Definition
System Description	Text used to identify the product name of this switch.
Machine Type	The machine model as defined by the Vital Product Data.
Machine Model	The machine model as defined by the Vital Product Data
Serial Number	The unique box serial number for this switch.
Part Number	Manufacturing part number.
Burned in MAC Address	Universally assigned network address.
Software Version	The release.version.revision number of the code currently running on the switch.
CPLD Version	The complex programmable logic device (CPLD) version.
Manufacturer Name	The name of the company who manufactured the switch.

Term	Definition
Revision	The revision number for the hardware.
Date Code	The date when the switch was manufactured, which is in YYYYMMDD format.
Operating System	The operating system currently running on the switch.
Network Processing Device	The type of the processor microcode.
Additional Packages	The additional packages incorporated into this system.

show platform vpd

This command displays vital product data for the switch.

Format	`show platform vpd`
Mode	User Privileged

The following information is displayed.

Term	Definition
Operational Code Image File Name	Build Signature loaded into the switch
Software Version	Release Version Maintenance Level and Build (RVMB) information of the switch.
Timestamp	Timestamp at which the image is built

The following shows example CLI display output for the command.

```
(CN1610) #show platform vpd

Operational Code Image File Name.............. FastPath-Ent-esw-
xgs4-gto-BL20R-CS-6AIQHSr3v7m14b35
Software Version.............................. 3.7.14.35
Timestamp..................................... Thu Mar  7 14:36:14
IST 2013
```

show interface

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

Format	`show interface {slot/port | switchport}`
Mode	Privileged EXEC

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

Parameters	**Definition**
Packets Received Without Error	The total number of packets (including broadcast packets and multicast packets) received by the processor.
Packets Received With Error	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Broadcast Packets Received	The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.
Receive Packets Discarded	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffered space.
Packets Transmitted Without Error	The total number of packets transmitted out of the interface.
Transmit Packets Discarded	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. A possible reason for discarding a packet could be to free up buffer space.
Transmit Packets Errors	The number of outbound packets that could not be transmitted because of errors.
Collisions Frames	The best estimate of the total number of collisions on this Ethernet segment.

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

The display parameters, when the argument is “switchport” are as follows:

Term	Definition
Packets Received Without Error	The total number of packets (including broadcast packets and multicast packets) received by the processor.
Broadcast Packets Received	The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.
Packets Received With Error	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Packets Transmitted Without Error	The total number of packets transmitted out of the interface.
Broadcast Packets Transmitted	The total number of packets that higher-level protocols requested to be transmitted to the Broadcast address, including those that were discarded or not sent.
Transmit Packet Errors	The number of outbound packets that could not be transmitted because of errors.
Time Since Counters Last Cleared	The elapsed time, in days, hours, minutes, and seconds since the statistics for this switch were last cleared.

show interfaces status

Use this command to display interface information, including the description, port state, speed and auto-neg capabilities. The command is similar to `show port all` but displays additional fields like interface description and port-capability.

The description of the interface is configurable through the existing command `description <name>` which has a maximum length of 64 characters that is truncated to 28 characters in the output. The long form of the description can be displayed using `show port description`. The interfaces displayed by this command are physical interfaces, LAG interfaces and VLAN routing interfaces.

Format	`show interfaces status [<slot/port>]`
Mode	Privileged EXEC

Field	Description
Port	The interface associated with the rest of the data in the row.
Name	The descriptive user-configured name for the interface.
Link State	Indicates whether the link is up or down.
Physical Mode	The speed and duplex settings on the interface.
Physical Status	Indicates the port speed and duplex mode for physical interfaces. The physical status for LAGs is not reported. When a port is down, the physical status is unknown.
Media Type	The media type of the interface.
Flow Control Status	The 802.3x flow control status.
Flow Control	The configured 802.3x flow control mode.

show interface counters

This command reports key summary statistics for all the ports (physical/CPU/port-channel).

Format	`show interface counters`
Mode	Privileged EXEC

Term	Definition
Port	The interface associated with the rest of the data in the row.
InOctects	The total number of octets received on the interface.
InUcastPkts	The total number of unicast packets received on the interface.
InMcastPkts	The total number of multicast packets received on the interface.
InBcastPkts	The total number of broadcast packets received on the interface.
OutOctects	The total number of octets transmitted by the interface.
OutUcastPkts	The total number of unicast packets transmitted by the interface.
OutMcastPkts	The total number of multicast packets transmitted by the interface.
OutBcastPkts	The total number of broadcast packets transmitted by the interface.

The following shows example CLI display output for the command.

```
(CN1610) #show interface counters

Port               InOctets      InUcastPkts      InMcastPkts
InBcastPkts
--------- ---------------- ---------------- ---------------- ------
----------

0/1                     0              0              0
0

Port               InOctets      InUcastPkts      InMcastPkts
InBcastPkts
--------- ---------------- ---------------- ---------------- ------
----------
0/1 0    0     0 0
0/2  0    0     0      0
```

```
0/3 150980         3139
0/4  000     0
0/5  000     0
...
...
ch1  0000
ch2  0000
...
ch64  0 000
CPU 3595330 3044217

Port             OutOctets     OutUcastPkts     OutMcastPkts
OutBcastPkts
--------- ---------------- ---------------- ---------------- ------
----------
0/1  0000
0/2 00 00
0/3 131369                0 1189
0/4  000 0
0/5  0000
...
...
ch1  0000
ch2  0000
...
ch64  0000
CPU 40252930 32910120
```

show interface ethernet

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

Format	`show interface ethernet {slot/port | switchport | all}`
Mode	Privileged EXEC

When you specify a value for slot/port, the command displays the following information.

Term	Definition
Packets Received	◆ **Total Packets Received (Octets)** - The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including Frame Check Sequence (FCS) octets). This object can be used as a reasonable estimate of Ethernet utilization. If greater precision is desired, the etherStatsPkts and etherStatsOctets objects should be sampled before and after a common interval. The result of this equation is the value Utilization which is the percent utilization of the Ethernet segment on a scale of 0 to 100 percent. ◆ **Packets Received 64 Octets** - The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets). ◆ **Packets Received 65–127 Octets** - The total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets). ◆ **Packets Received 128–255 Octets** - The total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).

Term	Definition
	◆ **Packets Received 256–511 Octets** - The total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets). ◆ **Packets Received 512–1023 Octets** - The total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets). ◆ **Packets Received 1024–1518 Octets** - The total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets). ◆ **Packets Received > 1518 Octets** - The total number of packets received that were longer than 1522 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.

Term	Definition
	◆ **Packets RX and TX 64 Octets** - The total number of packets (including bad packets) received and transmitted that were 64 octets in length (excluding framing bits but including FCS octets). ◆ **Packets RX and TX 65–127 Octets** - The total number of packets (including bad packets) received and transmitted that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets). ◆ **Packets RX and TX 128–255 Octets** - The total number of packets (including bad packets) received and transmitted that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets). ◆ **Packets RX and TX 256–511 Octets** - The total number of packets (including bad packets) received and transmitted that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).

Term	Definition
Packets Received (con't)	◆ **Packets RX and TX 512–1023 Octets** - The total number of packets (including bad packets) received and transmitted that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets). ◆ **Packets RX and TX 1024–1518 Octets** - The total number of packets (including bad packets) received and transmitted that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets). ◆ **Packets RX and TX 1519–2047 Octets** - The total number of packets received and transmitted that were between 1519 and 2047 octets in length inclusive (excluding framing bits, but including FCS octets) and were otherwise well formed. ◆ **Packets RX and TX 1523–2047 Octets** - The total number of packets received and transmitted that were between 1523 and 2047 octets in length inclusive (excluding framing bits, but including FCS octets) and were otherwise well formed. ◆ **Packets RX and TX 2048–4095 Octets** - The total number of packets received that were between 2048 and 4095 octets in length inclusive (excluding framing bits, but including FCS octets) and were otherwise well formed. ◆ **Packets RX and TX 4096–9216 Octets** - The total number of packets received that were between 4096 and 9216 octets in length inclusive (excluding framing bits, but including FCS octets) and were otherwise well formed.

Term	Definition
Packets Received Successfully	◆ **Total Packets Received Without Error** - The total number of packets received that were without errors. ◆ **Unicast Packets Received** - The number of subnetwork-unicast packets delivered to a higher-layer protocol. ◆ **Multicast Packets Received** - The total number of good packets received that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address. ◆ **Broadcast Packets Received** - The total number of good packets received that were directed to the broadcast address. Note that this does not include multicast packets.
Receive Packets Discarded	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.

Term	Definition
Packets Received with MAC Errors	◆ **Total Packets Received with MAC Errors** - The total number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol. ◆ **Jabbers Received** - The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). Note that this definition of jabber is different than the definition in IEEE-802.3 section 8.2.1.5 (10BASE5) and section 10.3.1.4 (10BASE2). These documents define jabber as the condition where any packet exceeds 20 ms. The allowed range to detect jabber is between 20 ms and 150 ms. ◆ **Fragments/Undersize Received** - The total number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets). ◆ **Alignment Errors** - The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with a non-integral number of octets. ◆ **FCS Errors -** The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with an integral number of octets. ◆ **Overruns** - The total number of frames discarded as this port was overloaded with incoming packets, and could not keep up with the inflow.

Term	Definition
Received Packets Not Forwarded	◆ **Total Received Packets Not Forwarded** - A count of valid frames received which were discarded (in other words, filtered) by the forwarding process ◆ **802.3x Pause Frames Received** - A count of MAC Control frames received on this interface with an opcode indicating the PAUSE operation. This counter does not increment when the interface is operating in half-duplex mode. ◆ **Unacceptable Frame Type** - The number of frames discarded from this port due to being an unacceptable frame type.

Term	Definition
Packets Transmitted Octets	◆ **Total Packets Transmitted (Octets)** - The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets). This object can be used as a reasonable estimate of Ethernet utilization. If greater precision is desired, the etherStatsPkts and etherStatsOctets objects should be sampled before and after a common interval. ----- ◆ **Packets Transmitted 64 Octets** - The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets). ◆ **Packets Transmitted 65-127 Octets** - The total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets). ◆ **Packets Transmitted 128-255 Octets** - The total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets). ◆ **Packets Transmitted 256-511 Octets** - The total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets). ◆ **Packets Transmitted 512-1023 Octets** - The total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets). ◆ **Packets Transmitted 1024-1518 Octets** - The total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets). ◆ **Packets Transmitted > 1518 Octets** - The total number of packets transmitted that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed. ◆ **Max Frame Size** - The maximum size of the

Term	Definition
Packets Transmitted Successfully	◆ **Total Packets Transmitted Successfully**- The number of frames that have been transmitted by this port to its segment. ◆ **Unicast Packets Transmitted** - The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent. ◆ **Multicast Packets Transmitted** - The total number of packets that higher-level protocols requested be transmitted to a Multicast address, including those that were discarded or not sent. ◆ **Broadcast Packets Transmitted** - The total number of packets that higher-level protocols requested be transmitted to the Broadcast address, including those that were discarded or not sent.
Transmit Packets Discarded	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. A possible reason for discarding a packet could be to free up buffer space.
Transmit Errors	◆ **Total Transmit Errors** - The sum of Single, Multiple, and Excessive Collisions. ◆ **FCS Errors** - The total number of packets transmitted that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with an integral number of octets. ◆ **Underrun Errors** - The total number of frames discarded because the transmit FIFO buffer became empty during frame transmission.

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

Term	Definition
Protocol Statistics	◆ **802.3x Pause Frames Transmitted** - A count of MAC Control frames transmitted on this interface with an opcode indicating the PAUSE operation. This counter does not increment when the interface is operating in half-duplex mode. ◆ **GVRP PDUs Received** - The count of GVRP PDUs received in the GARP layer. ◆ **GVRP PDUs Transmitted** - The count of GVRP PDUs transmitted from the GARP layer. ◆ **GVRP Failed Registrations** - The number of times attempted GVRP registrations could not be completed. ◆ **GMRP PDUs Received** - The count of GMRP PDUs received in the GARP layer. ◆ **GMRP PDUs Transmitted** - The count of GMRP PDUs transmitted from the GARP layer. ◆ **GMRP Failed Registrations** - The number of times attempted GMRP registrations could not be completed. ◆ **STP BPDUs Transmitted** - Spanning Tree Protocol Bridge Protocol Data Units sent. ◆ **STP BPDUs Received** - Spanning Tree Protocol Bridge Protocol Data Units received. ◆ **RST BPDUs Transmitted** - Rapid Spanning Tree Protocol Bridge Protocol Data Units sent. ◆ **RSTP BPDUs Received** - Rapid Spanning Tree Protocol Bridge Protocol Data Units received. ◆ **MSTP BPDUs Transmitted** - Multiple Spanning Tree Protocol Bridge Protocol Data Units sent. ◆ **MSTP BPDUs Received** - Multiple Spanning Tree Protocol Bridge Protocol Data Units received.

Term	Definition
Dot1x Statistics	◆ **EAPOL Frames Transmitted** - The number of EAPOL frames of any type that have been transmitted by this authenticator. ◆ **EAPOL Start Frames Received** - The number of valid EAPOL start frames that have been received by this authenticator.
Time Since Counters Last Cleared	The elapsed time, in days, hours, minutes, and seconds since the statistics for this port were last cleared.

If you use the `switchport` keyword, the following information appears.

Term	Definition
Packets Received Without Error	The total number of packets (including broadcast packets and multicast packets) received by the processor.
Broadcast Packets Received	The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.
Packets Received With Error	The total number of packets with errors (including broadcast packets and multicast packets) received by the processor.
Packets Transmitted without Errors	The total number of packets transmitted out of the interface.
Broadcast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to the Broadcast address, including those that were discarded or not sent.
Transmit Packet Errors	The number of outbound packets that could not be transmitted because of errors.
Time Since Counters Last Cleared	The elapsed time, in days, hours, minutes, and seconds, since the statistics for this switch were last cleared.

If you use the `all` keyword, the following information appears for all interfaces on the switch.

Term	Definition
Port	The Interface ID.
Bytes Tx	The total number of bytes transmitted by the interface.
Bytes Rx	The total number of bytes transmitted by the interface.
Packets Tx	The total number of packets transmitted by the interface.
Packets Rx	The total number of packets transmitted by the interface.

show interface ethernet switchport

This command displays the private VLAN mapping information for the switch interfaces.

Format	`show interface ethernet` *`interface-id`* `switchport`
Mode	Privileged EXEC

Parameter	Description
interface-id	The slot/port of the switch.

The command displays the following information.

Term	Definition
Private-vlan host-association	The VLAN association for the private-VLAN host ports.
Private-vlan mapping	The VLAN mapping for the private-VLAN promiscuous ports.

show interface lag

Use this command to display configuration information about the specified LAG interface.

Format	`show interface lag` *`lag-intf-num`*
Mode	Privileged EXEC

Parameters	Definition
Packets Received Without Error	The total number of packets (including broadcast packets and multicast packets) received on the LAG interface
Packets Received With Error	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Broadcast Packets Received	The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.
Receive Packets Discarded	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
Packets Transmitted Without Error	The total number of packets transmitted out of the LAG.
Transmit Packets Discarded	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. A possible reason for discarding a packet could be to free up buffer space.
Transmit Packets Errors	The number of outbound packets that could not be transmitted because of errors.
Collisions Frames	The best estimate of the total number of collisions on this Ethernet segment.

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

show fiber-ports optical-transceiver

This command displays the diagnostics information of the SFP like Temp, Voltage, Current, Input Power, Output Power, Tx Fault, and LOS. The values are derived from the SFP's A2 (Diagnostics) table using the I^2C interface.

Format	`show fiber-ports optical-transceiver {all | slot/port}`
Mode	Privileged EXEC

Field	Description
Temp	Internally measured transceiver temperature.
Voltage	Internally measured supply voltage.
Current	Measured TX bias current.
Output Power	Measured optical output power relative to 1mW.
Input Power	Measured optical power received relative to 1mW.
TX Fault	Transmitter fault.
LOS	Loss of signal.

The following information shows an example of the command output:

```
(CN1610) #show fiber-ports optical-transceiver all

                                        Output     Input
Port       Temp   Voltage   Current      Power     Power    TX      LOS
            [C]    [Volt]      [mA]      [dBm]     [dBm]   Fault
--------  -----  -------  -------    -------   -------   -----   ---
0/49       39.3     3.256       5.0    -2.234    -2.465   No      No
0/50       33.9     3.260       5.3    -2.374   -40.000   No      Yes
0/51       32.2     3.256       5.6    -2.300    -2.897   No      No
```

show fiber-ports optical-transceiver-info

This command displays the SFP vendor related information like Vendor Name, Serial Number of the SFP, Part Number of the SFP. The values are derived from the SFP's A0 table using the I^2C interface.

Format	`show fiber-ports optical-transceiver-info {all | slot/port}`
Mode	Privileged EXEC

Field	Description
Vendor Name	The vendor name is a 16 character field that contains ASCII characters, left-aligned and padded on the right with ASCII spaces (20h). The vendor name shall be the full name of the corporation, a commonly accepted abbreviation of the name of the corporation, the SCSI company code for the corporation, or the stock exchange code for the corporation.
Length (50um, OM2)	This value specifies link length that is supported by the transceiver while operating in compliance with applicable standards using 50 micron multimode OM2 [500MHz*km at 850nm] fiber. A value of zero means that the transceiver does not support 50 micron multimode fiber or that the length information must be determined from the transceiver technology.
Length (62.5um, OM1)	This value specifies link length that is supported by the transceiver while operating in compliance with applicable standards using 62.5 micron multimode OM1 [200 MHz*km at 850nm, 500 MHz*km at 1310nm] fiber. A value of zero means that the transceiver does not support 62.5 micron multimode fiber or that the length information must determined from the transceiver technology

Field	Description
Vendor SN	The vendor serial number (vendor SN) is a 16 character field that contains ASCII characters, left-aligned and padded on the right with ASCII spaces (20h), defining the vendor's serial number for the transceiver. A value of all zero in the 16-byte field indicates that the vendor SN is unspecified.
Vendor PN	The vendor part number (vendor PN) is a 16-byte field that contains ASCII characters, left aligned and added on the right with ASCII spaces (20h), defining the vendor part number or product name. A value of all zero in the 16-byte field indicates that the vendor PN is unspecified.
BR, nominal	The nominal bit (signaling) rate (BR, nominal) is specified in units of 100 MBd, rounded off to the nearest 100 MBd. The bit rate includes those bits necessary to encode and delimit the signal as well as those bits carrying data information. A value of 0 indicates that the bit rate is not specified and must be determined from the transceiver technology. The actual information transfer rate will depend on the encoding of the data, as defined by the encoding value.
Vendor Rev	The vendor revision number (vendor rev) contains ASCII characters, left aligned and padded on the right with ASCII spaces (20h), defining the vendor's product revision number. A value of all zero in this field indicates that the vendor revision is unspecified.

The following information shows an example of the command output:

```
(CN1610) #show fiber-ports optical-transceiver-info all

                                Link Link
Nominal
                            Length Length
Bit
```

```
                                50um 62.5um
Rate
Port     Vendor Name      [m] [m]  Serial Number    Part Number
[Mbps] Rev
-------- ---------------- --- ---- ---------------- ----------------
- ----- ----
0/49 BROADCOM 8    3 A7N2018414       AXM761           10300 10
0/51 BROADCOM 8    3 A7N2018472       AXM761           10300 10
0/52 BROADCOM 8    3 A7N2018501       AXM761           10300 10
```

show mac-addr-table

This command displays the forwarding database entries. These entries are used by the transparent bridging function to determine how to forward a received frame.

Enter `all` or no parameter to display the entire table. Enter a MAC Address and VLAN ID to display the table entry for the requested MAC address on the specified VLAN. Enter the *`count`* parameter to view summary information about the forwarding database table. Use the `interface` slot/port parameter to view MAC addresses on a specific interface.

Instead of slot/port, `lag` *`lag-intf-num`* can be used as an alternate way to specify the LAG interface. `lag` *`lag-intf-num`* can also be used to specify the LAG interface where *`lag-intf-num`* is the LAG port number. Use the `vlan` *`vlan_id`* parameter to display information about MAC addresses on a specified VLAN.

Format	`show mac-addr-table [{`*`macaddr vlan_id`* `| all | count | interface slot/port | vlan` *`vlan_id`*`}]`
Mode	Privileged EXEC

The following information displays if you do not enter a parameter, the keyword all, or the MAC address and VLAN ID.

Term	Definition
VLAN ID	The VLAN in which the MAC address is learned.

Term	Definition
MAC Address	A unicast MAC address for which the switch has forwarding and or filtering information. The format is 6 two-digit hexadecimal numbers that are separated by colons, for example *01:23:45:67:89:AB*.
Interface	The port through which this address was learned.
Interface Index	This object indicates the ifIndex of the interface table entry associated with this port.
Status	The status of this entry. The meanings of the values are: ◆ Static—The value of the corresponding instance was added by the system or a user when a static MAC filter was defined. It cannot be relearned. ◆ Learned—The value of the corresponding instance was learned by observing the source MAC addresses of incoming traffic, and is currently in use. ◆ Management—The value of the corresponding instance (system MAC address) is also the value of an existing instance of dot1dStaticAddress. It is identified with interface 0/1. and is currently used when enabling VLANs for routing. ◆ Self—The value of the corresponding instance is the address of one of the switch's physical interfaces (the system's own MAC address). ◆ GMRP Learned—The value of the corresponding was learned via GMRP and applies to Multicast. ◆ Other—The value of the corresponding instance does not fall into one of the other categories.

If you enter `vlan` *`vlan_id`*, only the MAC Address, Interface, and Status fields appear. If you enter the `interface` slot/port parameter, in addition to the MAC Address and Status fields, the VLAN ID field also appears.

The following information displays if you enter the `count` parameter:

Term	Definition
Dynamic Address count	Number of MAC addresses in the forwarding database that were automatically learned.
Static Address (User-defined) count	Number of MAC addresses in the forwarding database that were manually entered by a user.
Total MAC Addresses in use	Number of MAC addresses currently in the forwarding database.
Total MAC Addresses available	Number of MAC addresses the forwarding database can handle.

process cpu threshold

Use this command to configure the CPU utilization thresholds. The Rising and Falling thresholds are specified as a percentage of CPU resources. The utilization monitoring time period can be configured from 5 seconds to 86400 seconds in multiples of 5 seconds. The CPU utilization threshold configuration is saved across a switch reboot. Configuring the falling utilization threshold is optional. If the falling CPU utilization parameters are not configured, then they take the same value as the rising CPU utilization parameters.

Format	`process cpu threshold type total rising` *`1-100`* `interval`
Mode	Global Config

Parameter	Description
rising threshold	The percentage of CPU resources that, when exceeded for the configured rising interval, triggers a notification. The range is 1 to 100. The default is 0 (disabled).
rising interval	The duration of the CPU rising threshold violation, in seconds, that must be met to trigger a notification. The range is 5 to 86400. The default is 0 (disabled).

Parameter	Description
falling threshold	The percentage of CPU resources that, when usage falls below this level for the configured interval, triggers a notification. The range is 1 to 100. The default is 0 (disabled). A notification is triggered when the total CPU utilization falls below this level for a configured period of time. The falling utilization threshold notification is made only if a rising threshold notification was previously done. The falling utilization threshold must always be equal or less than the rising threshold value. The CLI does not allow setting the falling threshold to be greater than the rising threshold.
falling interval	The duration of the CPU falling threshold, in seconds, that must be met to trigger a notification. The range is 5 to 86400. The default is 0 (disabled).

show process app-list

This command displays the user and system applications.

Format	`show process app-list`
Mode	Privileged EXEC

Parameter	Description
ID	The application identifier.
Name	The name that identifies the process.
PID	The number the software uses to identify the process.
Admin Status	The administrative status of the process.
Auto Restart	Indicates whether the process will automatically restart if it stops.

Parameter	Description
Running Status	Indicates whether the process is currently running or stopped.

The following shows example CLI display output for the command.

```
                              Admin     Auto      Running
ID    Name            PID     Status    Restart   Status
----- --------------- ------- --------- --------- -------
   1 dataplane       15309 Enabled   Disabled  Running
   2 switchdrvr      15310 Enabled   Disabled  Running
   3 syncdb          15314 Enabled   Disabled  Running
   4 lighttpd        18718 Enabled   Enabled   Running
   5 syncdb-test         0 Disabled  Disabled  Stopped
   6 proctest            0 Disabled  Enabled   Stopped
   7 user.start          0 Enabled   Disabled  Stopped
```

show process app-resource-list

This command displays the configured and in-use resources of each application.

Format	`show process app-resource-list`
Mode	Privileged EXEC

Parameter	Description
ID	The application identifier.
Name	The name that identifies the process.
PID	The number the software uses to identify the process.
Memory Limit	The maximum amount of memory the process can consume.
CPU Share	The maximum percentage of CPU utilization the process can consume.
Memory Usage	The amount of memory the process is currently using.

Parameter	Description
Max Mem Usage	The maximum amount of memory the process has used at any given time since it started.

```
(CN1610) #show process app-resource-list

                                Memory      CPU       Memory      Max Mem
ID   Name               PID  Limit       Share     Usage       Usage
---- ---------------- ---- ----------- --------- ----------- ------
   1 switchdrvr        251   Unlimited Unlimited      380 MB 381 MB
   2 syncdb            252   Unlimited Unlimited        0 MB 0 MB
   3 syncdb-test         0   Unlimited Unlimited        0 MB 0 MB
   4 proctest            0       10 MB       20%        0 MB 0 MB
   5 utelnetd            0   Unlimited Unlimited        0 MB 0 MB
   6 lxshTelnetd         0   Unlimited Unlimited        0 MB 0 MB
   7 user.start          0   Unlimited Unlimited        0 MB 0 MB
```

show process cpu

This command provides the percentage utilization of the CPU by different tasks.

Note

It is not necessarily the traffic to the CPU, but different tasks that keep the CPU busy.

Format	`show process cpu [1-n | all]`
Mode	Privileged EXEC

Keyword	Description
Free	System wide free memory
Alloc	System wide allocated memory (excluding cache, file system used space)
Pid	Process or Thread Id
Name	Process or Thread Name
5Secs	CPU utilization sampling in 5Secs interval

Keyword	Description
60Secs	CPU utilization sampling in 60Secs interval
300Secs	CPU utilization sampling in 300Secs interval
TotalCPUUtilization	Total CPU utilization % within the specified window of 5Secs, 60Secs and 300Secs.

The following shows example CLI display output for the command using Linux.

```
(CN1610) #show process cpu
Memory Utilization Report
status      bytes
------ ----------
free    106450944
alloc   423227392

 CPU Utilization:

  PID      Name                    5 Secs     60 Secs    300 Secs
-----------------------------------------------------------------
  765    _interrupt_thread          0.00%       0.01%       0.02%
  767    bcmL2X.0                   0.58%       0.35%       0.28%
  768    bcmCNTR.0                  0.77%       0.73%       0.72%
  773    bcmRX                      0.00%       0.04%       0.05%
  786    cpuUtilMonitorTask         0.19%       0.23%       0.23%
  834    dot1s_task                 0.00%       0.01%       0.01%
  810    hapiRxTask                 0.00%       0.01%       0.01%
  805    dtlTask                    0.00%       0.02%       0.02%
  863    spmTask                    0.00%       0.01%       0.00%
  894    ip6MapLocalDataTask        0.00%       0.01%       0.01%
  908    RMONTask                   0.00%       0.11%       0.12%
-----------------------------------------------------------------
 Total CPU Utilization             1.55%       1.58%       1.50%
```

show process proc-list

This application displays the processes started by applications created by the Process Manager.

Format	`show process proc-list`
Mode	Privileged EXEC

Parameter	Description
PID	The number the software uses to identify the process.
Process Name	The name that identifies the process.
Application ID-Name	The application identifier and its associated name.
Child	Indicates whether the process has spawned a child process.
VM Size	Virtual memory size.
VM Peak	The maximum amount of virtual memory the process has used at a given time.
FD Count	The file descriptors count for the process.

The following shows example CLI display output for the command.

```
(CN1610) #show process proc-list

      Process         Application                VM Size  VM Peak
PID   Name           ID-Name              Chld  (KB)     (KB)    FD
Count
---- ---------------- -------------------- ---- -------- -------- -
15260 procmgr          0-procmgr             No       1984     1984 8
15309 dataplane        1-dataplane          No     293556   293560 11
15310 switchdrvr       2-switchdrvr         No     177220   177408 57
15314 syncdb           3-syncdb              No       2060     2080 8
```

show running-config

Use this command to display or capture the current setting of different protocol packages supported on the switch. This command displays or captures commands with settings and configurations that differ from the default value. To display or capture the commands with settings and configurations that are equal to the default value, include the `all` option.

Note

Show running-config does not display the User Password, even if you set one different from the default.

The output is displayed in script format, which can be used to configure another switch with the same configuration. If the optional *scriptname* is provided with a file name extension of ".scr", the output is redirected to a script file.

Note

If you issue the `show running-config` command from a serial connection, access to the switch through remote connections (such as Telnet) is suspended while the output is being generated and displayed.

Note

If you use a text-based configuration file, the `show running-config` command only displays configured physical interfaces (i.e. if any interface only contains the default configuration, that interface will be skipped from the `show running-config` command output). This is true for any configuration mode that contains nothing but default configuration. That is, the command to enter a particular config mode, followed immediately by its exit command, are both omitted from the `show running-config` command output (and hence from the startup-config file when the system configuration is saved.)

Use the following keys to navigate the command output.

Key	Action
Enter	Advance one line.
Space Bar	Advance one page.
q	Stop the output and return to the prompt.

Note that `--More-- or (q)uit` is displayed at the bottom of the output screen until you reach the end of the output.

This command captures the current settings of OSPFv2 and OSPFv3 trapflag status:

- If all the flags are enabled, then the command displays `trapflags all`.
- If all the flags in a particular group are enabled, then the command displays `trapflags group name all`.
- If some, but not all, of the flags in that group are enabled, the command displays `trapflags groupname flag-name`.

Format	`show running-config [all | scriptname]`

Mode	Privileged EXEC

show running-config interface

Use this command to display the running configuration for a specific interface. Valid interfaces include physical, LAG, and VLAN interfaces.

Format	`show running-config interface {`*`interface`*` | lag {`*`lag-intf-num`*`} | vlan {`*`vlan-id`*`}}`
Mode	Privileged EXEC

Parameter	Description
interface	Running configuration for the specified interface.
lag-intf-num	Running configuration for the LAG interface.
vlan-id	Running configuration for the VLAN routing interface.

The following information is displayed for the command.

Parameter	Description
unit|slot	Enter an interface in unit/slot/port format.
lag	Display the running config for a specified lag interface.
vlan	Display the running config for a specified vlan routing interface.

The following shows example CLI display output for the command.

```
(CN1610) #show running-config interface 0/1
!Current Configuration:
!
interface  0/1
addport 3/1
exit
(CN1610) #
```

show

This command displays the content of text-based configuration files from the CLI. The text-based configuration files (startup-config, backup-config and factory-defaults) are saved compressed in flash. With this command, the files are decompressed while displaying their content.

Format	`show { startup-config | backup-config | factory-defaults }`
Mode	Privileged EXEC

Parameter	Description
startup-config	Display the content of the startup-config file.
backup-config	Display the content of the backup-config file.
factory-defaults	Display the content of the factory-defaults file.

The following shows example CLI display output for the command using the startup-config parameter.

```
(CN1610) #show startup-config
!Current Configuration:
!
!System Description "Quanta LB6M, 8.1.14.41, Linux 2.6.27.47, U-
Boot 2009.06 (Apr 19 2011 - 15:57:06)"
!System Software Version "8.1.14.41"
!System Up Time          "0 days 0 hrs 48 mins 19 secs"
!Additional Packages     BGP-4,QOS,IPv6,IPv6
Management,Routing,Data Center
!Current SNTP Synchronized Time: Not Synchronized
!
vlan database
vlan 10
exit
configure
ipv6 router ospf
exit
line console
exit
line telnet
exit
line ssh
exit

!
```

```
--More-- or (q)uit
interface 0/1
description 'intf1'
exit
router ospf
exit
exit
```

The following shows example CLI display output for the command using the backup-config parameter.

```
(CN1610) #show backup-config
!Current Configuration:
!
!System Description "Quanta LB6M, 8.1.14.41, Linux 2.6.27.47, U-
Boot 2009.06 (Apr 19 2011 - 15:57:06)"
!System Software Version "8.1.14.41"
!System Up Time          "0 days 0 hrs 48 mins 19 secs"
!Additional Packages     BGP-4,QOS,IPv6,IPv6
Management,Routing,Data Center
!Current SNTP Synchronized Time: Not Synchronized
!
vlan database
vlan 10
exit
configure
ipv6 router ospf
exit
line console
exit
line telnet
exit
line ssh
exit
!
--More-- or (q)uit
interface 0/1
description 'intf1'
exit
router ospf
exit
exit
```

The following shows example CLI display output for the command using the factory-defaults parameter.

```
(CN1610) #show factory-defaults
!Current Configuration:
!
```

```
!System Description "Quanta LB6M, 8.1.14.41, Linux 2.6.27.47, U-
Boot 2009.06 (Apr 19 2011 - 15:57:06)"
!System Software Version "8.1.14.41"
!System Up Time          "0 days 0 hrs 48 mins 19 secs"
!Additional Packages     BGP-4,QOS,IPv6,IPv6
Management,Routing,Data Center
!Current SNTP Synchronized Time: Not Synchronized
!
vlan database
vlan 10
exit
configure
ipv6 router ospf
exit
line console
exit
line telnet
exit
line ssh
exit
!
--More-- or (q)uit
interface 0/1
description 'intf1'
exit
router ospf
exit
exit
```

dir

Use this command to list the files in the directory /mnt/fastpath in flash from the CLI.

Format	dir
Mode	Privileged EXEC

```
(CN1610) #dir

    0  drwx                2048 May 09 2002 16:47:30 .
    0  drwx                2048 May 09 2002 16:45:28 ..
    0  -rwx                 592 May 09 2002 14:50:24 slog2.txt
    0  -rwx                  72 May 09 2002 16:45:28 boot.dim
    0  -rwx                   0 May 09 2002 14:46:36 olog2.txt
    0  -rwx            13376020 May 09 2002 14:49:10 image1
    0  -rwx                   0 Apr 06 2001 19:58:28 fsyssize
```

```
    0   -rwx                1776 May 09 2002 16:44:38 slog1.txt
    0   -rwx                 356 Jun 17 2001 10:43:18 crashdump.ctl
    0   -rwx                1024 May 09 2002 16:45:44 sslt.rnd
    0   -rwx            14328276 May 09 2002 16:01:06 image2
    0   -rwx                 148 May 09 2002 16:46:06 hpc_broad.cfg
    0   -rwx                   0 May 09 2002 14:51:28 olog1.txt
    0   -rwx                 517 Jul 23 2001 17:24:00 ssh_host_key
    0   -rwx               69040 Jun 17 2001 10:43:04
log_error_crashdump
    0   -rwx                 891 Apr 08 2000 11:14:28 sslt_key1.pem
    0   -rwx                 887 Jul 23 2001 17:24:00
ssh_host_rsa_key
    0   -rwx                 668 Jul 23 2001 17:24:34
ssh_host_dsa_key
    0   -rwx                 156 Apr 26 2001 13:57:46 dh512.pem
    0   -rwx                 245 Apr 26 2001 13:57:46 dh1024.pem
    0   -rwx                   0 May 09 2002 16:45:30 slog0.txt
```

show sysinfo

This command displays switch information.

Format	`show sysinfo`
Mode	Privileged EXEC

Term	Definition
Switch Description	Text used to identify this switch.
System Name	Name used to identify the switch.The factory default is blank. To configure the system name, see “snmp-server” on page 89.
System Location	Text used to identify the location of the switch. The factory default is blank. To configure the system location, see “snmp-server” on page 89.
System Contact	Text used to identify a contact person for this switch. The factory default is blank. To configure the system location, see “snmp-server” on page 89.
System ObjectID	The base object ID for the switch’s enterprise MIB.

Term	Definition
System Up Time	The time in days, hours and minutes since the last switch reboot.
Current SNTP Synchronized Time	The system time acquired from a network SNTP server.
MIBs Supported	A list of MIBs supported by this agent.

show tech-support

Use the `show tech-support` command to display system and configuration information when you contact technical support. The output of the `show tech-support` command combines the output of the following commands and includes log history files from previous runs:

- show version
- show sysinfo
- show hardware
- show interface ethernet switchport
- show port all
- show process cpu
- show mbuf total
- show platform vpd
- show mac-addr-table
- show debugging
- show vlan brief
- show vlan port all
- show port-channel all
- show spanning-tree
- show logging
- show logging buffered
- show logging persistent
- show logging persistent previous
- show running-config
- debug crash & kernel logs

Format	`show tech-support`

Mode	Privileged EXEC

length *value*

Use this command to set the pagination length to value number of lines for the sessions specified by configuring on different Line Config modes (telnet/ssh/console) and is persistent.

Length command on Line Console mode applies for Serial Console session.

Default	`24`
Format	`length value`
Mode	Line Config

no length *value*

Use this command to set the pagination length to the default value number of lines.

Format	`no length value`
Mode	Line Config

terminal length

Use this command to set the pagination length to *value* number of lines for the current session. This command configuration takes an immediate effect on the current session and is nonpersistent.

Default	24 lines per page
Format	`terminal length value`
Mode	Privileged EXEC

no terminal length

Use this command to set the *value* to the length value configured on Line Config mode depending on the type of session.

Format	`no terminal length value`
Mode	Privileged EXEC

show terminal length

Use this command to display all the configured terminal length values.

Format	`show terminal length`
Mode	Privileged EXEC

The following shows example CLI display output for the command.

```
(CN1610) #show terminal length
Terminal Length:
----------------------
For Current Session…….. 24
For Serial Console…… 24
For Telnet Sessions……... 24
For SSH Sessions…….. 24
```

memory free low-watermark processor

Use this command to get notifications when the CPU free memory falls below the configured threshold. A notification is generated when the free memory falls below the threshold. Another notification is generated once the available free memory rises to 10 percent above the specified threshold. To prevent generation of excessive notifications when the CPU free memory fluctuates around the configured threshold, only one Rising or Falling memory notification is generated over a period of 60 seconds. The threshold is specified in kilobytes. The CPU free memory threshold configuration is saved across a switch reboot.

Format	`memory free low-watermark processor` *1-515916*
Mode	Global Config

Parameter	Description
low-watermark	When CPU free memory falls below this threshold, a notification message is triggered. The range is 1 to the maximum available memory on the switch. The default is 0 (disabled).

Box Services Commands

This section describes the Box Services commands. Box services are services that provide support for features such as temperature, power supply status, fan control, and others. Each of these services is platform dependent. (For example, some platforms may have temperature sensors, but no fan controller. Or, others may have both while others have neither.)

Note
The bootloader version can only be supported on PowerPC platforms that use the u-boot loader.

environment trap

Use this command to configure environment status traps.

Format	`environment trap {fan|powersupply|temperature}`
Mode	Global Config

Parameter	Definition
fan	Enables or disables the sending of traps for fan status events. The default is enable.
powersupply	Enables or disables the sending of traps for power supply status events. The default is enable.
temperature	Enables or disables the sending of traps for temperature status events. The default is enable.

show environment

Use this command to view information about the switch environment.

Format	`show environment`
Mode	Privileged Exec

Term	Definition
Temp	The current temperature of the switch environment, in Celsius.
Fan Speed	The current speed of the fan, in RPM.
Fan Duty Level	
Temperature traps range	The minimum and maximum temperatures for normal operation, in Celsius.
Temperature Sensors	Shows information for each switch temperature sensor.
Unit	The unit number for the switch.
Sensor	The number of the temperature sensor on the unit.
Description	A description of the temperature sensor.
Temp	The current temperature of the sensor.
State	The current state of the sensor.
Max_Temp	The maximum temperature reached by this sensor.
Fans	Shows information for each fan on the switch.
Unit	The unit number for the switch.
Fan	The number of the fan on the unit.
Description	A description of the fan.
Type	The type of fan.
Speed	The current speed of the fan, in RPM.
Duty Level	The current duty level for the fan.
State	The current state of the fan.
Power Modules	Shows information for each power module in the switch.
Unit	The unit number for the switch.

Term	Definition
Power Supply	The number of the power supply in the unit.
Description	A description of the power module.
Type	The type of power module.
State	The current state of the power module.

The following shows example CLI display output for the command.

```
(CN1610) #show environment

Temp (C)..................................... 36
Fan Speed, RPM............................... 12840
Fan Duty Level............................... 100%
Temperature traps range: 0 to 60 degrees (Celsius)

Temperature Sensors:
Unit     Sensor  Description       Temp (C)    State
Max_Temp (C)
----     ------  ----------------  ----------  ----------- -------
1        1       CPU & SWITCH      33          Normal          33
1        2       Left PHY's        34          Normal          35
1        3       Right PHY's       36          Normal          37

Fans:
Unit Fan Description  Type      Speed Duty level    State
---- --- -----------  --------  ----- ------------- -----------
1    1   Fan-1        Removable 12840 100%          Operational
1    2   Fan-2        Removable 12600 100%          Operational
1    3   Fan-3        Removable 12660 100%          Operational
1    4   Fan-4        Removable 12660 100%          Operational

Power Modules:
Unit     Power supply   Description        Type          State
----     ------------   ----------------   ----------   -----------
1        1              Internal AC-1      Removable    Operational
1        2              Internal AC-2      Removable    Not powered
```

show hardware

This command displays inventory information for the switch.

Format	show hardware

Mode	Privileged EXEC

Term	Definition
System Description	Text used to identify the product name of this switch.
Machine Type	The machine model as defined by the Vital Product Data.
Machine Model	The machine model as defined by the Vital Product Data
Serial Number	The unique box serial number for this switch.
Part Number	Manufacturing part number.
Burned in MAC Address	Universally assigned network address.
Software Version	The release.version.revision number of the code currently running on the switch.
CPLD Version	The complex programmable logic device (CPLD) version.
Manufacturer Name	The name of the company who manufactured the switch.
Revision	The revision number for the hardware.
Date Code	The date when the switch was manufactured, which is in YYYYMMDD format.
Operating System	The operating system currently running on the switch.
Network Processing Device	The type of the processor microcode.
Additional Packages	The additional packages incorporated into this system.
Power Supply Hardware Data	

Term	Definition
Unit	The switch unit number in which the power supply is installed, which is always 1.
Power Supply	The power supply identifier.
State	Indicates whether the power supply is installed.
Part Number & Revision	The power supply part number and revision.
Mfg Part Number & Revision	The power supply part number assigned by the manufacturer and its revision number.
Serial Number	The serial number of the power supply.
Date Code	The date when the power supply was manufactured, which is in YYYYMMDD format.
Fan Tray Hardware Detail	
Unit	The switch unit number in which the fan tray is installed, which is always 1.
Fan Tray	The fan tray identifier.
State	Indicates whether the fan tray is installed.
Part Number and Rev	The fan tray part number and revision.
SFP Module Hardware Data	
Status of SFP Module	Indicates whether one of more SFP modules is installed.
SFP Vendor	The name of the company who made the SFP module.
SFP Part Number	The vendor-assigned part number for the SFP.
SFP Serial Number	The serial number of the SFP module.

The following shows example CLI display output for the command.

```
(CN1610) #show hardware

Switch: 1
```

```
System Description..... NetApp CN1610,
1.2.0.0, Linux 3.8.13-4ce360e8
Machine Type..... NetApp CN1610
Machine Model..... CN1610
Serial Number..... 40811200201
Part Number..... 111-00982
Burned In MAC Address..... 00:A0:98:EA:2E:7A
Software Version..... 1.2.0.0
CPLD version..... 0x6
Manufacturer Name..... NetApp, Inc.
Revision..... E0
Date Code..... 20140824
Operating System.....Linux 3.8.13-4ce360e8
Network Processing Device..... BCM56820_B0
Additional Packages..... FASTPATH QOS
                         FASTPATH IPv6
Management

Power Supply Hardware Data:

      Power               Part Number       Mfg Part Number                    Date
Unit  supply  State        & Revision        & Revision        Serial Number    Code
----  ------  -----------  ----------------  ----------------  ---------------  -----
1     1       Present      114-00098+A0      DPSN-300DB H.00   DHUD1432008017   20140809
1     2       Present      114-00098+A0      DPSN-300DB H.00   DHUD1432008021   20140809

Fan Tray Hardware Data:

Unit  Fan Tray  State        Part Number & Rev
----  --------  -----------  -------------------
1     1         Present      441-00033
1     2         Present      441-00033
1     3         Present      441-00033
1     4         Present      441-00033

SFP Module Hardware Data:

No SFP(s) / Fiberport(s) available
```

Logging Commands

This section describes the commands you use to configure system logging, and to view logs and the logging settings.

logging buffered

This command enables logging to an in-memory log.

Default	disabled; critical when enabled
Format	`logging buffered`
Mode	Global Config

no logging buffered

This command disables logging to in-memory log.

Format	`no logging buffered`
Mode	Global Config

logging buffered wrap

This command enables wrapping of in-memory logging when the log file reaches full capacity. Otherwise when the log file reaches full capacity, logging stops.

Default	enabled
Format	`logging buffered wrap`
Mode	Privileged EXEC

no logging buffered wrap

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

Format	`no logging buffered wrap`
Mode	Privileged EXEC

logging cli-command

This command enables the CLI command logging feature, which enables the FASTPATH software to log all CLI commands issued on the system. The commands are stored in a persistent log. Use the "show logging persistent" on page 199 command to display the stored history of CLI commands.

Default	enabled
Format	`logging cli-command`
Mode	Global Config

no logging cli-command

This command disables the CLI command Logging feature.

Format	`no logging cli-command`
Mode	Global Config

logging console

This command enables logging to the console. You can specify the *severitylevel* value as either an integer from 0 to 7 or symbolically through one of the following keywords: `emergency (0), alert (1), critical (2), error (3), warning (4), notice (5), info (6), or debug (7).`

Default	disabled; critical when enabled
Format	`logging console` *[severitylevel]*
Mode	Global Config

no logging console

This command disables logging to the console.

Format	`no logging console`
Mode	Global Config

logging host

This command configures the logging host parameters. You can configure up to eight hosts.

Default	◆ port—514 ◆ level—critical (2)
Format	`logging host {`*`hostaddress`*`|`*`hostname`*`} `*`addresstype {port severitylevel}`*
Mode	Global Config

Parameter	Description
hostaddress|hostname	The IP address of the logging host.
address-type	Indicates the type of address ipv4 or ipv6 or dns being passed.
port	A port number from 1 to 65535.
severitylevel	Specify this value as either an integer from 0 to 7, or symbolically through one of the following keywords: `emergency` (0), `alert` (1), `critical` (2), `error` (3), `warning` (4), `notice` (5), `info` (6), or `debug` (7).

The following shows examples of the command.

```
(CN1610) (Config)# logging host google.com dns 214
(CN1610) (Config)# logging host 10.130.64.88 ipv4 214 6
(CN1610) (Config)# logging host 2000::150 ipv6 214 7
```

logging host reconfigure

This command enables logging host reconfiguration.

Format	`logging host reconfigure `*`hostindex`*
Mode	Global Config

Parameter	Description
hostindex	Enter the Logging Host Index for which to change the IP address.

logging host remove

This command disables logging to host. See “show logging hosts” on page 198 for a list of host indexes.

Format	`logging host remove` *`hostindex`*
Mode	Global Config

logging syslog

This command enables syslog logging.

Format	`logging syslog`
Mode	Global Config

no logging syslog

This command disables syslog logging.

Format	`no logging syslog`
Mode	Global Config

logging syslog port

This command enables syslog logging. The *`portid`* parameter is an integer with a range of 1-65535.

Default	disabled
Format	`logging syslog port` *`portid`*
Mode	Global Config

no logging syslog port

This command disables syslog logging.

Format	`no logging syslog port`
Mode	Global Config

show logging

This command displays logging configuration information.

Format	`show logging`
Mode	Privileged EXEC

Term	Definition
Logging Client Local Port	Port on the collector/relay to which syslog messages are sent.
Logging Client Source Interface	Shows the configured syslog source-interface (source IP address).
CLI Command Logging	Shows whether CLI Command logging is enabled.
Console Logging	Shows whether console logging is enabled.
Console Logging Severity Filter	The minimum severity to log to the console log. Messages with an equal or lower numerical severity are logged.
Buffered Logging	Shows whether buffered logging is enabled.
Persistent Logging	Shows whether persistent logging is enabled.
Persistent Logging Severity Filter	The minimum severity at which the logging entries are retained after a system reboot.
Syslog Logging	Shows whether syslog logging is enabled.
Log Messages Received	Number of messages received by the log process. This includes messages that are dropped or ignored.
Log Messages Dropped	Number of messages that could not be processed due to error or lack of resources.
Log Messages Relayed	Number of messages sent to the collector/relay.

The following shows example CLI display output for the command.

```
(CN1610) #show logging

Logging Client Local Port           : 514
Logging Client Source Interface     : (not configured)
```

```
CLI Command Logging                 : disabled
Console Logging                     : enabled
Console Logging Severity Filter     : error
Buffered Logging                    : enabled
Persistent Logging                  : disabled
Persistent Logging Severity Filter  : alert

Syslog Logging                      : disabled

Log Messages Received               : 1010
Log Messages Dropped                : 0
Log Messages Relayed                : 0
```

show logging buffered

This command displays buffered logging (system startup and system operation logs).

Format	`show logging buffered`
Mode	Privileged EXEC

Term	Definition
Buffered (In-Memory) Logging	Shows whether the In-Memory log is enabled or disabled.
Buffered Logging Wrapping Behavior	The behavior of the In Memory log when faced with a log full situation.
Buffered Log Count	The count of valid entries in the buffered log.

show logging hosts

This command displays all configured logging hosts. Use the "|" character to display the output filter options.

Format	`show logging hosts`
Mode	Privileged EXEC

Term	Definition
Host Index	(Used for deleting hosts.)
IP Address / Hostname	IP address or hostname of the logging host.
Severity Level	The minimum severity to log to the specified address. The possible values are emergency (0), alert (1), critical (2), error (3), warning (4), notice (5), info (6), or debug (7).
Port	The server port number, which is the port on the local host from which syslog messages are sent.
Host Status	Status field provides the current status of snmp row status. (Active, Not in Service, Not Ready).

The following shows example CLI display output for the command.

```
(CN1610) #show logging hosts ?

<cr>                      Press enter to execute the command.
|                         Output filter options.

(CN1610) #show logging hosts

Index  IP Address/Hostname       Severity   Port   Status
-------- ---------------------- -----------  ------ ---------
1         10.130.64.88 critical     514    Active
2         2000::150 critical     514    Active
```

show logging persistent

Use the **show logging persistent** command to display persistent log entries. If `log-files` is specified, the system persistent log files are displayed.

Format	`show logging persistent [log-files]`
Mode	Privileged EXEC

Parameter	Description
Persistent Logging	If persistent logging is enabled or disabled.

Parameter	Description
Persistent Log Count	The number of persistent log entries.
Persistent Log Files	The list of persistent log files in the system. Only displayed if `log-files` is specified.

The following shows example CLI display output for the command.

```
(Broadcom FASTPATH Switching) #show logging persistent

Persistent Logging: disabled
Persistent Log Count: 0

(Broadcom FASTPATH Switching) #show logging persistent log-files

Persistent Log Files:

slog0.txt
slog1.txt
slog2.txt
olog0.txt
olog1.txt
olog2.txt
```

show logging traplogs

This command displays SNMP trap events and statistics.

Format	`show logging traplogs`
Mode	Privileged EXEC

Term	Definition
Number of Traps Since Last Reset	The number of traps since the last boot.
Trap Log Capacity	The number of traps the system can retain.
Number of Traps Since Log Last Viewed	The number of new traps since the command was last executed.

Term	Definition
Log	The log number.
System Time Up	How long the system had been running at the time the trap was sent.
Trap	The text of the trap message.

clear logging buffered

This command clears buffered logging (system startup and system operation logs).

Format	`clear logging buffered`
Mode	Privileged EXEC

Email Alerting and Mail Server Commands

logging email

This command enables email alerting and sets the lowest severity level for which log messages are emailed. If you specify a severity level, log messages at or above this severity level, but below the urgent severity level, are emailed in a non-urgent manner by collecting them together until the log time expires. You can specify the *severitylevel* value as either an integer from 0 to 7 or symbolically through one of the following keywords: `emergency` (0), `alert` (1), `critical` (2), `error` (3), `warning` (4), `notice` (5), `info` (6), or `debug` (7).

Default	disabled; when enabled, log messages at or above severity Warning (4) are emailed
Format	`logging email` *[severitylevel]*
Mode	Global Config

no logging email

This command disables email alerting.

Format	`no logging email`
Mode	Global Config

logging email urgent

This command sets the lowest severity level at which log messages are emailed immediately in a single email message. Specify the *severitylevel* value as either an integer from 0 to 7 or symbolically through one of the following keywords: `emergency (0), alert (1), critical (2), error (3), warning (4), notice (5), info (6), or debug (7)`. Specify `none` to indicate that log messages are collected and sent in a batch email at a specified interval.

Default	Alert (1) and emergency (0) messages are sent immediately.
Format	`logging email urgent {`*severitylevel* `| none}`
Mode	Global Config

no logging email urgent

This command resets the urgent severity level to the default value.

Format	`no logging email urgent`
Mode	Global Config

logging email message-type to-addr

This command configures the email address to which messages are sent. The message types supported are `urgent, non-urgent`, and `both`. For each supported severity level, multiple email addresses can be configured. The *`to-email-addr`* variable is a standard email address, for example admin@yourcompany.com.

Format	`logging email message-type {urgent |non-urgent |both} to-addr` *`to-email-addr`*
Mode	Global Config

no logging email message-type to-addr

This command removes the configured to-addr field of email.

Format	`no logging email message-type {urgent |non-urgent |both} to-addr` *`to-email-addr`*
Mode	Global Config

logging email from-addr

This command configures the email address of the sender (the switch).

Default	switch@broadcom.com
Format	`logging email from-addr` *`from-email-addr`*
Mode	Global Config

no logging email from-addr

This command removes the configured email source address.

Format	`no logging email from-addr` *`from-email-addr`*
Mode	Global Config

logging email message-type subject

This command configures the subject line of the email for the specified type.

Default	For urgent messages: Urgent Log Messages For non-urgent messages: Non Urgent Log Messages
Format	`logging email message-type {urgent |non-urgent |both} subject` *`subject`*
Mode	Global Config

no logging email message-type subject

This command removes the configured email subject for the specified message type and restores it to the default email subject.

Format	`no logging email message-type {urgent |non-urgent |both} subject`
Mode	Global Config

logging email logtime

This command configures how frequently non-urgent email messages are sent. Non-urgent messages are collected and sent in a batch email at the specified interval. The valid range is every 30–1440 minutes.

Default	30 minutes
Format	`logging email logtime` *`minutes`*
Mode	Global Config

no logging email logtime

This command resets the non-urgent log time to the default value.

Format	`no logging email logtime`
Mode	Global Config

logging traps

This command sets the severity at which SNMP traps are logged and sent in an email. Specify the *severitylevel* value as either an integer from 0 to 7 or symbolically through one of the following keywords: `emergency` (0), `alert` (1), `critical` (2), `error` (3), `warning` (4), `notice` (5), `info` (6), or `debug` (7).

Default	Info (6) messages and higher are logged.
Format	`logging traps` *severitylevel*
Mode	Global Config

no logging traps

This command resets the SNMP trap logging severity level to the default value.

Format	`no logging traps`
Mode	Global Config

logging email test message-type

This command sends an email to the SMTP server to test the email alerting function.

Format	`logging email test message-type {urgent |non-urgent |both} message-body` *message-body*
Mode	Global Config

show logging email config

This command displays information about the email alert configuration.

Format	`show logging email config`
Mode	Privileged EXEC

Term	Definition
Email Alert Logging	The administrative status of the feature: enabled or disabled

Term	Definition
Email Alert From Address	The email address of the sender (the switch).
Email Alert Urgent Severity Level	The lowest severity level that is considered urgent. Messages of this type are sent immediately.
Email Alert Non Urgent Severity Level	The lowest severity level that is considered non-urgent. Messages of this type, up to the urgent level, are collected and sent in a batch email. Log messages that are less severe are not sent in an email message at all.
Email Alert Trap Severity Level	The lowest severity level at which traps are logged.
Email Alert Notification Period	The amount of time to wait between non-urgent messages.
Email Alert To Address Table	The configured email recipients.
Email Alert Subject Table	The subject lines included in urgent (Type 1) and non-urgent (Type 2) messages.
For Msg Type urgent, subject is	The configured email subject for sending urgent messages.
For Msg Type non-urgent, subject is	The configured email subject for sending non-urgent messages.

show logging email statistics

This command displays email alerting statistics.

Format	`show logging email statistics`
Mode	Privileged EXEC

Term	Definition
Email Alert Operation Status	The operational status of the email alerting feature.
No of Email Failures	The number of email messages that have attempted to be sent but were unsuccessful.
No of Email Sent	The number of email messages that were sent from the switch since the counter was cleared.
Time Since Last Email Sent	The amount of time that has passed since the last email was sent from the switch.

clear logging email statistics

This command resets the email alerting statistics.

Format	`clear logging email statistics`
Mode	Privileged EXEC

mail-server

This command configures the SMTP server to which the switch sends email alert messages and changes the mode to Mail Server Configuration mode. The server address can be in the IPv4, IPv6, or DNS name format.

Format	`mail-server {`*`ip-address`* `|` *`ipv6-address`* `|` *`hostname`*`}`
Mode	Global Config

no mail-server

This command removes the specified SMTP server from the configuration.

Format	`no mail-server {`*`ip-address`* `|` *`ipv6-address`* `|` *`hostname`*`}`
Mode	Global Config

security

This command sets the email alerting security protocol by enabling the switch to use TLS authentication with the SMTP Server. If the TLS mode is enabled on the switch but the SMTP sever does not support TLS mode, no email is sent to the SMTP server.

Default	none
Format	`security {tlsv1 | none}`
Mode	Mail Server Config

port

This command configures the TCP port to use for communication with the SMTP server. The recommended port for TLSv1 is 465, and for no security (i.e. none) it is 25. However, any nonstandard port in the range 1 to 65535 is also allowed.

Default	25
Format	`port {465 | 25 | 1-65535}`
Mode	Mail Server Config

username (Mail Server Config)

This command configures the login ID the switch uses to authenticate with the SMTP server.

Default	admin
Format	`username` *`name`*
Mode	Mail Server Config

password

This command configures the password the switch uses to authenticate with the SMTP server.

Default	admin
Format	`password` *`password`*
Mode	Mail Server Config

show mail-server config

This command displays information about the email alert configuration.

Format	`show mail-server {`*`ip-address`* `|` *`hostname`* `| all} config`
Mode	Privileged EXEC

Term	Definition
No of mail servers configured	The number of SMTP servers configured on the switch.
Email Alert Mail Server Address	The IPv4/IPv6 address or DNS hostname of the configured SMTP server.
Email Alert Mail Server Port	The TCP port the switch uses to send email to the SMTP server
Email Alert Security Protocol	The security protocol (TLS or none) the switch uses to authenticate with the SMTP server.
Email Alert Username	The username the switch uses to authenticate with the SMTP server.
Email Alert Password	The password the switch uses to authenticate with the SMTP server.

System Utility and Clear Commands

This section describes the commands you use to help troubleshoot connectivity issues and to restore various configurations to their factory defaults.

traceroute

Use the `traceroute` command to discover the routes that IPv4 or IPv6 packets actually take when traveling to their destination through the network on a hop-by-hop basis. Traceroute continues to provide a synchronous response when initiated from the CLI.

The user may specify the source IP address or the virtual router of the traceroute probes. Recall that traceroute works by sending packets that are expected not to reach their final destination, but instead trigger ICMP error messages back to the source address from each hop along the forward path to the destination. By specifying the source address, the user can determine where along the forward path there is no route back to the source address. Note that this is only useful if the route from source to destination and destination to source is symmetric.) It would be common, for example, to send a traceroute from an edge router to a target higher in the network using a source address from a host subnet on the edge router. This would test reachability from within the network back to hosts attached to the edge router..

In the CLI, the user may specify the source as an IPv4 address, IPv6 address, a virtual router, or as a routing interface. When the source is specified as a routing interface, the traceroute is sent using the primary IPv4 address on the source interface. With SNMP, the source must be specified as an address.

CN1610 will not accept an incoming packet, such as a traceroute response, that arrives on a routing interface if the packet's destination address is on one of the out-of-band management interfaces (service port or network port). Similarly, CN1610 will not accept a packet that arrives on a management interface if the packet's destination is an address on a routing interface. Thus, it would be futile to send a traceroute on a management interface using a routing interface address as source, or to send a traceroute on a routing interface using a management interface as source. When sending a traceroute on a routing interface, the source must be that routing interface or another routing interface. When sending a traceroute on a management interface, the source must be on that management interface. For this reason, the user cannot specify the source as a management interface or management interface address. When sending a traceroute on a management interface, the user should not specify a source address, but instead let the system select the source address from the outgoing interface.

Default	◆ count: 3 probes ◆ interval: 3 seconds ◆ size: 0 bytes ◆ port: 33434 ◆ maxTtl: 30 hops ◆ maxFail: 5 probes ◆ initTtl: 1 hop
Format	`traceroute [vrf vrf-name] {ip-address | [ipv6] {ipv6-address | hostname}} [initTtl initTtl] [maxTtl maxTtl] [maxFail maxFail] [interval interval] [count count] [port port] [size size] [source {ip-address | | ipv6-address | unit/slot/port}]`
Mode	Privileged EXEC

Using the options described below, you can specify the initial and maximum time-to-live (TTL) in probe packets, the maximum number of failures before termination, the number of probes sent for each TTL, and the size of each probe.

Parameter	**Description**
vrf-name	The name of the VRF instance from which to initiate traceroute. Only hosts reachable from within the VRF instance can be tracerouted. If a source parameter is specified in conjunction with a vrf parameter, it must be a member of the VRF. The ipv6 parameter cannot be used in conjunction with the vrf parameter.
ipaddress	The *ipaddress* value should be a valid IP address.
ipv6-address	The *ipv6-address* value should be a valid IPv6 address.
hostname	The *hostname* value should be a valid hostname.
ipv6	The optional *ipv6* keyword can be used before *ipv6-address* or *hostname*. Giving the *ipv6* keyword before the *hostname* tries it to resolve to an IPv6 address.

Parameter	Description
initTtl	Use *initTtl* to specify the initial time-to-live (TTL), the maximum number of router hops between the local and remote system. Range is 0 to 255.
maxTtl	Use *maxTtle* to specify the maximum TTL. Range is 1 to 255.
maxFail	Use *maxFail* to terminate the traceroute after failing to receive a response for this number of consecutive probes. Range is 0 to 255.
interval	Use the optional *interval* parameter to specify the time between probes, in seconds. If a response is not received within this interval, then traceroute considers that probe a failure (printing *) and sends the next probe. If traceroute does receive a response to a probe within this interval, then it sends the next probe immediately. Range is 1 to 60 seconds.
count	Use the optional *count* parameter to specify the number of probes to send for each TTL value. Range is 1 to 10 probes.
port	Use the optional *port* parameter to specify destination UDP port of the probe. This should be an unused port on the remote destination system. Range is 1 to 65535.
size	Use the optional *size* parameter to specify the size, in bytes, of the payload of the Echo Requests sent. Range is 0 to 65507 bytes.
source	Use the optional *source* parameter to specify the source IP address or interface for the traceroute.

The following are examples of the CLI command.

traceroute Success:

```
(CN1610) # traceroute 10.240.10.115 initTtl 1 maxTtl 4 maxFail 0
interval 1 count 3 port 33434 size 43
```

```
 Traceroute to 10.240.10.115 ,4 hops max 43 byte packets:
1 10.240.4.1   708 msec     41 msec     11 msec
2 10.240.10.115   0 msec     0 msec     0 msec

Hop Count = 1 Last TTL = 2 Test attempt = 6 Test Success = 6
```

traceroute ipv6 Success

```
(CN1610) # traceroute 2001::2 initTtl 1 maxTtl 4 maxFail 0 interval
1 count 3 port 33434 size 43

Traceroute to 2001::2 hops max 43 byte packets:
1 2001::2   708 msec     41 msec     11 msec

The above command can also be execute with the optional ipv6
parameter as follows:

(CN1610) # traceroute ipv6 2001::2 initTtl 1 maxTtl 4 maxFail 0
interval 1 count 3 port 33434 size 43
```

traceroute Failure:

```
(CN1610) # traceroute 10.40.1.1 initTtl 1 maxFail 0 interval 1
count 3
port 33434 size 43
Traceroute to 10.40.1.1 ,30 hops max 43 byte packets:
1 10.240.4.1   19 msec     18 msec     9 msec
2 10.240.1.252   0 msec     0 msec     1 msec
3 172.31.0.9   277 msec     276 msec     277 msec
4 10.254.1.1   289 msec     327 msec     282 msec
5 10.254.21.2   287 msec     293 msec     296 msec
6 192.168.76.2   290 msec     291 msec     289 msec
7 0.0.0.0   0 msec *
Hop Count = 6 Last TTL = 7 Test attempt = 19 Test Success = 18
```

traceroute ipv6 Failure

```
(CN1610)# traceroute 2001::2 initTtl 1 maxFail 0 interval 1 count 3
port 33434 size 43

Traceroute to 2001::2 hops max 43 byte packets:
1 3001::1   708 msec     41 msec     11 msec
2 4001::2   250 msec     200 msec    193 msec
3 5001::3   289 msec     313 msec    278 msec
4 6001::4   651 msec     41 msec     270 msec
5          0             0 msec *
Hop Count = 4 Last TTL = 5 Test attempt = 1 Test Success = 0
```

clear config

This command resets the configuration to the factory defaults without powering off the switch. When you issue this command, a prompt appears to confirm that the reset should proceed. When you enter y, you automatically reset the current configuration on the switch to the default values. It does not reset the switch.

Format	`clear config`
Mode	Privileged EXEC

clear counters

This command clears the statistics for a specified slot/port, for all the ports, or for the entire switch based upon the argument. If a virtual router is specified, the statistics for the ports on the virtual router are cleared. If no router is specified, the information for the default router will be displayed.

Format	`clear counters {slot/port | all [vrf` *`vrf-name`*`]}`
Mode	Privileged EXEC

clear igmpsnooping

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

Format	`clear igmpsnooping`
Mode	Privileged EXEC

clear pass

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

Format	`clear pass`
Mode	Privileged EXEC

clear traplog

This command clears the trap log.

Format	`clear traplog`

Mode	Privileged EXEC

clear vlan

This command resets VLAN configuration parameters to the factory defaults. When the VLAN configuration is reset to the factory defaults, there are some scenarios regarding GVRP and MVRP that happen due to this:

1. Static VLANs are deleted.
2. GVRP is restored to the factory default as a result of handling the VLAN RESTORE NOTIFY event. Since GVRP is disabled by default, this means that GVRP should be disabled and all of its dynamic VLANs should be deleted.
3. MVRP is restored to the factory default as a result of handling the VLAN RESTORE NOTIFY event. Since MVRP is enabled by default, this means that any VLANs already created by MVRP are unaffected. However, for customer platforms where MVRP is disabled by default, then the MVRP behavior should match GVRP. That is, MVRP is disabled and the MVRP VLANs are deleted.

Format	`clear vlan`
Mode	Privileged EXEC

logout

This command closes the current telnet connection or resets the current serial connection.

Note
Save configuration changes before logging out.

Format	`logout`
Modes	◆ Privileged EXEC ◆ User EXEC

ping

Use this command to determine whether another computer is on the network. Ping provides a synchronous response when initiated from the CLI.

Note

For information about the `ping` command for IPv6 hosts, see “ping ipv6” on page 601.

Default	◆ The default count is 1. ◆ The default interval is 3 seconds. ◆ The default size is 0 bytes.
Format	`ping [vrf vrf-name] {address| hostname | {ipv6 {interface {unit/slot/port | vlan 1-4093 | network | serviceport} link-local-address} | ipv6-address | hostname} [count count] [interval 1-60] [size size] [source ip-address | ipv6-address | {unit/slot/port | vlan 1-4093 | serviceport | network}]`
Modes	◆ Privileged EXEC ◆ User EXEC

Using the options described below, you can specify the number and size of Echo Requests and the interval between Echo Requests.

Parameter	Description
vrf-name	The name of the virtual router in which to initiate the ping. If no virtual router is specified, the ping is initiated in the default router instance.
address	IPv4 or IPv6 addresses to ping.
count	Use the `count` parameter to specify the number of ping packets (ICMP Echo requests) that are sent to the destination address specified by the *ip-address* field. The range for *count* is 1 to 15 requests.
interval	Use the `interval` parameter to specify the time between Echo Requests, in seconds. Range is 1 to 60 seconds.
size	Use the `size` parameter to specify the size, in bytes, of the payload of the Echo Requests sent. Range is 0 to 65507 bytes.

Parameter	Description
source	Use the *source* parameter to specify the source IP/IPv6 address or interface to use when sending the Echo requests packets.
hostname	Use the *hostname* parameter to resolve to an IPv4 or IPv6 address. The *ipv6* keyword is specified to resolve the hostname to IPv6 address. The IPv4 address is resolved if no keyword is specified.
ipv6	The optional keyword *ipv6* can be used before the *ipv6-address* or *hostname* argument. Using the *ipv6* optional keyword before *hostname* tries to resolve it directly to the IPv6 address. Also used for pinging a link-local IPv6 address.
interface	Use the *interface* keyword to ping a link-local IPv6 address over an interface.
link-local-address	The link-local IPv6 address to ping over an interface.

The following are examples of the CLI command.

IPv4 ping success:

```
(CN1610) #ping 10.254.2.160 count 3 interval 1 size 255
Pinging 10.254.2.160 with 255 bytes of data:

Received response for icmp_seq = 0. time = 275268 usec
Received response for icmp_seq = 1. time = 274009 usec
Received response for icmp_seq = 2. time = 279459 usec

----10.254.2.160 PING statistics----
3 packets transmitted, 3 packets received, 0% packet loss
round-trip (msec) min/avg/max = 274/279/276
```

IPv6 ping success

```
(CN1610) #ping 2001::1
 Pinging 2001::1 with 64 bytes of data:

Send count=3, Receive count=3 from 2001::1
Average round trip time = 3.00 ms
```

IPv4 ping failure:

In Case of Unreachable Destination:

```
(CN1610) # ping 192.168.254.222 count 3 interval 1 size 255
Pinging 192.168.254.222 with 255 bytes of data:
Received Response: Unreachable Destination
Received Response :Unreachable Destination
Received Response :Unreachable Destination
----192.168.254.222  PING statistics----
3 packets transmitted,3 packets received, 0% packet loss
round-trip (msec) min/avg/max = 0/0/0
```

In Case Of Request TimedOut:

```
(CN1610) # ping 1.1.1.1 count 1 interval 3
Pinging 1.1.1.1 with 0 bytes of data:

----1.1.1.1 PING statistics----
1 packets transmitted,0 packets received, 100% packet loss
round-trip (msec) min/avg/max = 0/0/0
```

IPv6 ping failure

```
(CN1610) #ping ipv6 2001::4
 Pinging 2001::4 with 64 bytes of data:

Send count=3, Receive count=0 from 2001::4
Average round trip time = 0.00 ms
```

quit

This command closes the current telnet connection or resets the current serial connection. The system asks you whether to save configuration changes before quitting.

Format	`quit`
Modes	◆ Privileged EXEC ◆ User EXEC

reload

This command resets the switch without powering it off. Reset means that all network connections are terminated and the boot code executes. The switch uses the stored configuration to initialize the switch. You are prompted to confirm that the reset should proceed. The LEDs on the switch indicate a successful reset.

Format	`reload`

Mode	Privileged EXEC

copy

The copy command uploads and downloads files to and from the switch. You can also use the copy command to manage the dual images (active and backup) on the file system. Upload and download files from a server using FTP, TFTP, Xmodem, Ymodem, or Zmodem. SFTP and SCP are available as additional transfer methods if the software package supports secure management. If FTP is used, a password is required.

Format	copy *source destination* {verify | noverify}
Mode	Privileged EXEC

Replace the *source* and *destination* parameters with the desired options. For the *url* source or destination, use one of the following values:
{xmodem | tftp://*ipaddr*|*hostname* | *ip6address*|*hostname/filepath/filename* [noval]| sftp|scp://*username@ipaddr* | *ipv6address/filepath/filename* | ftp://*user@ipaddress* | *hostname/filepath/filename*}

verify|*noverify* is only available if the image/configuration verify options feature is enabled (see "write memory" on page 224). verify specifies that digital signature verification will be performed for the specified downloaded image or configuration file. noverify specifies that no verification will be performed.

The keyword **ias-users** supports the downloading of the IAS user database file. When the IAS users file is downloaded, the switch IAS user's database is replaced with the users and its attributes available in the downloaded file. In the command **copy *url* ias-users**, for *url* one of the following is used for IAS users file:

{ { tftp://<ipaddr|hostname>|<ipv6address|hostname>/<filepath>/<filename> } | { sftp|scp://<username>@<ipaddress>/<filepath>/<filename>} }

Note

The maximum length for the file path is 160 characters, and the maximum length for the file name is 31 characters.

For FTP, TFTP, SFTP and SCP, the *ipaddr|hostname* parameter is the IP address or host name of the server, *filepath* is the path to the file, and *filename* is the name of the file you want to upload or download. For SFTP and SCP, the *username* parameter is the username for logging into the remote server via SSH.

Note

ip6address is also a valid parameter for routing packages that support IPv6.

To copy OpenFlow SSL certificates to the switch using TFTP or XMODEM, using only the following options pertinent to the OpenFlow SSL certificates.

Format	`copy [<mode/file>] nvram:{openflow-ssl-ca-cert | openflow-ssl-cert | openflow-ssl-priv-key}`
Mode	Privileged EXEC

CAUTION

Remember to upload the existing fastpath.cfg file off the switch prior to loading a new release image in order to make a backup.

Source	Destination	Description
`nvram:application:` *`sourcefilename`*	*`url`*	Filename of source application file.
`nvram:backup-config`	`nvram:startup-config`	Copies the backup configuration to the startup configuration.
`nvram:clibanner`	*`url`*	Copies the CLI banner to a server.

Source	Destination	Description
nvram: core-dump	tftp://<ipaddress|hostname>/<filepath>/<filename>| ftp://<user>@<ipaddr|hostname>/<path>/<filename> | scp://<user>@<ipaddr|hostname>/<path>/<filename> | sftp://<user>@<ipaddr|hostname>/<path>/<filename>}	Uploads the core dump file on the local system to an external TFTP/FTP/SCP/SFTP server.
nvram:cpupktcapture.pcap	*url*	Uploads CPU packets capture file.
nvram:crash-log	url	Copies the crash log to a server.
nvram:errorlog	*url*	Copies the error log file to a server.
nvram:factory-defaults	*url*	Uploads factory defaults file.
nvram:fastpath.cfg	*url*	Uploads the binary config file to a server.
nvram:log	*url*	Copies the log file to a server.
nvram:operational-log	url	Copies the operational log file to a server.
nvram:script *scriptname*	*url*	Copies a specified configuration script file to a server.
nvram:startup-config	nvram:backup-config	Copies the startup configuration to the backup configuration.
nvram:startup-config	*url*	Copies the startup configuration to a server.

Source	Destination	Description
nvram:startup-log	url	Uploads the startup log file.
nvram:traplog	*url*	Copies the trap log file to a server.
system:running-config	nvram:startup-config	Saves the running configuration to NVRAM.
system:running-config	nvram:factory-defaults	Saves the running configuration to NVRAM to the *factory-defaults* file.
system:image	url	Saves the system image to a server.
url	nvram:application *destfilename*	Destination file name for the application file.
url	nvram:clibanner	Downloads the CLI banner to the system.
url	nvram:fastpath.cfg	Downloads the binary config file to the system.
url	nvram:publickey-config	Downloads the Public Key for Configuration Script validation.
url	nvram:publickey-image	Downloads Public Key for Image validation.
url	nvram:script *destfilename*	Downloads a configuration script file to the system. During the download of a configuration script, the copy command validates the script. In case of any error, the command lists all the lines at the end of the validation process and prompts you to confirm before copying the script file.
url	nvram:script *destfilename* noval	When you use this option, the copy command will not validate the downloaded script file. An example of the CLI command follows:

Source	Destination	Description
`(CN1610) #copy tftp://1.1.1.1/file.scr nvram:script file.scr noval`		
url	`nvram:sshkey-dsa`	Downloads an SSH key file. For more information, see "Secure Shell Commands" on page 47.
url	`nvram:sshkey-rsa1`	Downloads an SSH key file.
url	`nvram:sshkey-rsa2`	Downloads an SSH key file.
url	`nvram:startup-config`	Downloads the startup configuration file to the system.
url	`ias-users`	Downloads an IAS users database file to the system. When the IAS users file is downloaded, the switch IAS user's database is replaced with the users and their attributes available in the downloaded file.
url	`{active | backup}`	Download an image from the remote server to either image.
`{active | backup}`	*url*	Upload either image to the remote server.
`active`	`backup`	Copy the active image to the backup image.
`backup`	`active`	Copy the backup image to the active image.

The following shows an example of downloading and applying ias users file.

```
(CN1610) #copy tftp://10.131.17.104/aaa_users.txt ias-users

Mode..................................... TFTP
Set Server IP............................ 10.131.17.104
Path..................................... ./
Filename................................. aaa_users.txt
Data Type................................ IAS Users
```

```
Management access will be blocked for the duration of the transfer
Are you sure you want to start? (y/n) y

File transfer operation completed successfully.

Validating and updating the users to the IAS users database.


Updated IAS users database successfully.


(CN1610) #
```

write memory

Use this command to save running configuration changes to NVRAM so that the changes you make will persist across a reboot. This command is the same as `copy system:running-config nvram:startup-config`. Use the `confirm` keyword to directly save the configuration to NVRAM without prompting for a confirmation.

Format	`write memory [confirm]`
Mode	Privileged EXEC

Simple Network Time Protocol Commands

This section describes the commands you use to automatically configure the system time and date by using Simple Network Time Protocol (SNTP).

sntp broadcast client poll-interval

This command sets the poll interval for SNTP broadcast clients in seconds as a power of two where *poll-interval* can be a value from 6 to 10.

Default	6
Format	`sntp broadcast client poll-interval` *poll-interval*
Mode	Global Config

no sntp broadcast client poll-interval

This command resets the poll interval for SNTP broadcast client back to the default value.

Format	`no sntp broadcast client poll-interval`
Mode	Global Config

sntp client mode

This command enables Simple Network Time Protocol (SNTP) client mode and may set the mode to either broadcast or unicast.

Default	disabled
Format	`sntp client mode [`*broadcast* `|` *unicast*`]`
Mode	Global Config

no sntp client mode

This command disables Simple Network Time Protocol (SNTP) client mode.

Format	`no sntp client mode`
Mode	Global Config

sntp client port

This command sets the SNTP client port ID to 0, 123 or a value between 1025 and 65535. The default value is 0, which means that the SNTP port is not configured by the user. In the default case, the actual client port value used in SNTP packets is assigned by the underlying OS.

Default	0
Format	`sntp client port` *`portid`*
Mode	Global Config

no sntp client port

This command resets the SNTP client port back to its default value.

Format	`no sntp client port`
Mode	Global Config

sntp unicast client poll-interval

This command sets the poll interval for SNTP unicast clients in seconds as a power of two where *`poll-interval`* can be a value from 6 to 10.

Default	6
Format	`sntp unicast client poll-interval` *`poll-interval`*
Mode	Global Config

no sntp unicast client poll-interval

This command resets the poll interval for SNTP unicast clients to its default value.

Format	`no sntp unicast client poll-interval`
Mode	Global Config

sntp unicast client poll-timeout

This command sets the poll timeout for SNTP unicast clients in seconds to a value from 1-30.

Default	5

Format	`sntp unicast client poll-timeout` *`poll-timeout`*
Mode	Global Config

no sntp unicast client poll-timeout

This command will reset the poll timeout for SNTP unicast clients to its default value.

Format	`no sntp unicast client poll-timeout`
Mode	Global Config

sntp unicast client poll-retry

This command will set the poll retry for SNTP unicast clients to a value from 0 to 10.

Default	1
Format	`sntp unicast client poll-retry` *`poll-retry`*
Mode	Global Config

no sntp unicast client poll-retry

This command will reset the poll retry for SNTP unicast clients to its default value.

Format	`no sntp unicast client poll-retry`
Mode	Global Config

sntp server

This command configures an SNTP server (a maximum of three). The server address can be either an IPv4 address or an IPv6 address. The optional priority can be a value of 1-3, the version a value of 1-4, and the port id a value of 1-65535.

Format	`sntp server {`*`ipaddress`* `|` *`ipv6address`* `|` *`hostname`*`} [`*`priority`* `[`*`version`* `[`*`portid`*`]]`
Mode	Global Config

no sntp server

This command deletes an server from the configured SNTP servers.

Format	`no sntp server remove {`*`ipaddress`* `|` *`ipv6address`* `|` *`hostname`*`}`
Mode	Global Config

show sntp

This command is used to display SNTP settings and status.

Format	`show sntp`
Mode	Privileged EXEC

Term	Definition
Last Update Time	Time of last clock update.
Last Attempt Time	Time of last transmit query (in unicast mode).
Last Attempt Status	Status of the last SNTP request (in unicast mode) or unsolicited message (in broadcast mode).
Broadcast Count	Current number of unsolicited broadcast messages that have been received and processed by the SNTP client since last reboot.

show sntp client

This command is used to display SNTP client settings.

Format	`show sntp client`
Mode	Privileged EXEC

Term	Definition
Client Supported Modes	Supported SNTP Modes (Broadcast or Unicast).
SNTP Version	The highest SNTP version the client supports.

Term	Definition
Port	SNTP Client Port. The field displays the value 0 if it is default value. When the client port value is 0, if the client is in broadcast mode, it binds to port 123; if the client is in unicast mode, it binds to the port assigned by the underlying OS.
Client Mode	Configured SNTP Client Mode.

show sntp server

This command is used to display SNTP server settings and configured servers.

Format	`show sntp server`
Mode	Privileged EXEC

Term	Definition
Server Host Address	IP address or hostname of configured SNTP Server.
Server Type	Address type of server (IPv4, IPv6, or DNS).
Server Stratum	Claimed stratum of the server for the last received valid packet.
Server Reference ID	Reference clock identifier of the server for the last received valid packet.
Server Mode	SNTP Server mode.
Server Maximum Entries	Total number of SNTP Servers allowed.
Server Current Entries	Total number of SNTP configured.

For each configured server:

Term	Definition
IP Address / Hostname	IP address or hostname of configured SNTP Server.

Term	Definition
Address Type	Address Type of configured SNTP server (IPv4, IPv6, or DNS).
Priority	IP priority type of the configured server.
Version	SNTP Version number of the server. The protocol version used to query the server in unicast mode.
Port	Server Port Number.
Last Attempt Time	Last server attempt time for the specified server.
Last Update Status	Last server attempt status for the server.
Total Unicast Requests	Number of requests to the server.
Failed Unicast Requests	Number of failed requests from server.

Time Zone Commands

Use the Time Zone commands to configure system time and date, Time Zone and Summer Time (that is, Daylight Saving Time). Summer time can be recurring or non-recurring.

clock set

This command sets the system time and date.

Format	`clock set` *`hh:mm:ss`* `clock set` *`mm/dd/yyyy`*
Mode	Global Config

Parameter	Description
hh:mm:ss	Enter the current system time in 24-hour format in hours, minutes, and seconds. The range is hours: 0 to 23, minutes: 0 to 59, seconds: 0 to 59.
mm/dd/yyyy	Enter the current system date the format month, day, year. The range for month is 1 to 12. The range for the day of the month is 1 to 31. The range for year is 2010 to 2079.

The following shows examples of the command.

```
(CN1610) (Config)# clock set 03:17:00

(CN1610) (Config)# clock set 11/01/2011
```

clock summer-time date

Use the clock summer-time date command to set the summer-time offset to Coordinated Universal Time (UTC). If the optional parameters are not specified, they are read as either **0** or **\0**, as appropriate.

Format	clock summer-time date {*date month year hh:mm date month year hh:mm*}[offset *offset*] [zone *acronym*]
Mode	Global Config

Parameter	Description
date	Day of the month. Range is 1 to 31.
month	Month. Range is the first three letters by name; jan, for example.
year	Year. The range is 2000 to 2097.
hh:mm	Time in 24-hour format in hours and minutes. The range is hours: 0 to 23, minutes: 0 to 59.
offset	The number of minutes to add during the summertime. The range is 1 to 1440.
acronym	The acronym for the summer-time to be displayed when summertime is in effect. The range is up to four characters are allowed.

The following shows examples of the command.

```
(CN1610) (Config)# clock summer-time date 1 nov 2011 3:18 2 nov
2011 3:18
(CN1610) (Config)# clock summer-time date 1 nov 2011 3:18 2 nov
2011 3:18 offset 120 zone INDA
```

clock summer-time recurring

This command sets the summer-time recurring parameters.

Format	clock summer-time recurring {*week day month hh:mm week day month hh:mm*} [offset *offset*] [zone *acronym*]
Mode	Global Config

Parameter	Description
EU	The system clock uses the standard recurring summer time settings used in countries in the European Union.

Parameter	Description
USA	The system clock uses the standard recurring daylight saving time settings used in the United States.
week	Week of the month. The range is 1 to 5, first, last.)
day	Day of the week. The range is the first three letters by name; sun, for example.
month	Month. The range is the first three letters by name; jan, for example.
hh:mm	Time in 24-hour format in hours and minutes. The range is hours: 0 to 23, minutes: 0 to 59.
offset	The number of minutes to add during the summertime. The range is 1 to 1440.
acronym	The acronym for the summertime to be displayed when summertime is in effect. Up to four characters are allowed.

The following shows examples of the command.

```
(CN1610) (Config)# clock summer-time recurring 2 sun nov 3:18 2 mon
nov 3:18
(CN1610) (Config)# clock summer-time recurring 2 sun nov 3:18 2 mon
nov 3:18 offset 120 zone INDA
```

no clock summer-time

This command disables the summer-time settings.

Format	no clock summer-time
Mode	Global Config

The following shows an example of the command.

```
(CN1610) (Config)# no clock summer-time
```

clock timezone

Use this command to set the offset to Coordinated Universal Time (UTC). If the optional parameters are not specified, they will be read as either **0** or **\0** as appropriate.

Format	clock timezone {*hours*} [minutes *minutes*] [zone *acronym*]
Mode	Global Config

Parameter	**Description**
hours	Hours difference from UTC. The range is -12 to +13.
minutes	Minutes difference from UTC. The range is 0 to 59.
acronym	The acronym for the time zone. The range is up to four characters.

The following shows an example of the command.

```
(CN1610) (Config)# clock timezone 5 minutes 30 zone INDA
```

no clock timezone

Use this command to reset the time zone settings.

Format	no clock timezone
Mode	Global Config

The following shows an example of the command.

```
(CN1610) (Config)# no clock timezone
```

show clock

Use this command to display the time and date from the system clock.

Format	show clock
Mode	Privileged EXEC

The following shows example CLI display output for the command.

```
(CN1610) # show clock
```

```
15:02:09 (UTC+0:00) Nov 1 2011
No time source
```

The following shows example CLI display output for the command.

With the above configuration the output appears as below:

```
(CN1610) # show clock

10:55:40 INDA(UTC+7:30) Nov 1 2011
No time source
```

show clock detail

Use this command to display the detailed system time along with the time zone and the summertime configuration.

Format	show clock detail
Mode	Privileged EXEC

The following shows example CLI display output for the command.

```
(CN1610) # show clock detail

15:05:24 (UTC+0:00) Nov 1 2011
No time source

Time zone:
Acronym not configured
Offset is UTC+0:00

Summertime:
Summer-time is disabled
```

The following shows example CLI display output for the command.

With the above configuration the output appears as below:

```
(CN1610) # show clock detail

10:57:57 INDA(UTC+7:30) Nov 1 2011
No time source

 Time zone:
 Acronym is INDA
 Offset is UTC+5:30
```

```
Summertime:
Acronym is INDA
Recurring every year
Begins on second Sunday of Nov at 03:18
Ends on second Monday of Nov at 03:18
Offset is 120 minutes
Summer-time is in effect.
```

DNS Client Commands

These commands are used in the Domain Name System (DNS), an Internet directory service. DNS is how domain names are translated into IP addresses. When enabled, the DNS client provides a hostname lookup service to other components of FASTPATH.

ip domain lookup

Use this command to enable the DNS client.

Default	enabled
Format	`ip domain lookup`
Mode	Global Config

no ip domain lookup

Use this command to disable the DNS client.

Format	`no ip domain lookup`
Mode	Global Config

ip domain name

Use this command to define a default domain name that FASTPATH software uses to complete unqualified host names (names with a domain name). By default, no default domain name is configured in the system. *`name`* may not be longer than 255 characters and should not include an initial period. This *`name`* should be used only when the default domain name list, configured using the `ip domain list command,` is empty.

Default	none
Format	`ip domain name` *`name`*
Mode	Global Config

The CLI command `ip domain name yahoo.com` will configure yahoo.com as a default domain name. For an unqualified hostname xxx, a DNS query is made to find the IP address corresponding to xxx.yahoo.com.

no ip domain name

Use this command to remove the default domain name configured using the `ip domain name` command.

Format	`no ip domain name`
Mode	Global Config

ip domain list

Use this command to define a list of default domain names to complete unqualified names. By default, the list is empty. Each name must be no more than 256 characters, and should not include an initial period. The default domain name, configured using the `ip domain name` command, is used only when the default domain name list is empty. A maximum of 32 names can be entered in to this list.

Default	none
Format	`ip domain list` *`name`*
Mode	Global Config

no ip domain list

Use this command to delete a name from a list.

Format	`no ip domain list` *`name`*
Mode	Global Config

ip name server

Use this command to configure the available name servers. Up to eight servers can be defined in one command or by using multiple commands. The parameter *`server-address`* is a valid IPv4 or IPv6 address of the server. The preference of the servers is determined by the order they were entered.

Format	`ip name-server` *`server-address1`* [*`server-address2...server-address8`*]
Mode	Global Config

no ip name server

Use this command to remove a name server.

Format	`no ip name-server [server-address1...server-address8]`
Mode	Global Config

ip host

Use this command to define static host name-to-address mapping in the host cache. The parameter *name* is host name and *ip address* is the IP address of the host. The hostname can include 1–255 alphanumeric characters, periods, hyphens, underscores, and non-consecutive spaces. Hostnames that include one or more space must be enclosed in quotation marks, for example “lab-pc 45”.

Default	none
Format	`ip host name ipaddress`
Mode	Global Config

no ip host

Use this command to remove the name-to-address mapping.

Format	`no ip host name`
Mode	Global Config

ipv6 host

Use this command to define static host name-to-IPv6 address mapping in the host cache. The parameter *name* is host name and *v6 address* is the IPv6 address of the host. The hostname can include 1–255 alphanumeric characters, periods, hyphens, and spaces. Hostnames that include one or more space must be enclosed in quotation marks, for example “lab-pc 45”.

Default	none
Format	`ipv6 host name v6 address`
Mode	Global Config

no ipv6 host

Use this command to remove the static host name-to-IPv6 address mapping in the host cache.

Format	`no ipv6 host` *`name`*
Mode	Global Config

ip domain retry

Use this command to specify the number of times to retry sending Domain Name System (DNS) queries. The parameter *`number`* indicates the number of times to retry sending a DNS query to the DNS server. This number ranges from 0 to 100.

Default	2
Format	`ip domain retry` *`number`*
Mode	Global Config

no ip domain retry

Use this command to return to the default.

Format	`no ip domain retry` *`number`*
Mode	Global Config

ip domain timeout

Use this command to specify the amount of time to wait for a response to a DNS query. The parameter *`seconds`* specifies the time, in seconds, to wait for a response to a DNS query. The parameter *`seconds`* ranges from 0 to 3600.

Default	3
Format	`ip domain timeout` *`seconds`*
Mode	Global Config

no ip domain timeout

Use this command to return to the default setting.

Format	`no ip domain timeout` *`seconds`*

Mode	Global Config

clear host

Use this command to delete entries from the host name-to-address cache. This command clears the entries from the DNS cache maintained by the software. This command clears both IPv4 and IPv6 entries.

Format	`clear host {name | all}`
Mode	Privileged EXEC

Field	Description
name	A particular host entry to remove. The parameter *name* ranges from 1-255 characters.
all	Removes all entries.

show hosts

Use this command to display the default domain name, a list of name server hosts, the static and the cached list of host names and addresses. The parameter *name* ranges from 1-255 characters. This command displays both IPv4 and IPv6 entries.

Format	`show hosts [name]`
Mode	Privileged EXEC User EXEC

Field	Description
Host Name	Domain host name.
Default Domain	Default domain name.
Default Domain List	Default domain list.
Domain Name Lookup	DNS client enabled/disabled.

Field	Description
Number of Retries	Number of time to retry sending Domain Name System (DNS) queries.
Retry Timeout Period	Amount of time to wait for a response to a DNS query.
Name Servers	Configured name servers.
DNS Client Source Interface	Shows the configured source interface (source IP address) used for a DNS client. The IP address of the selected interface is used as source IP for all communications with the server.

The following shows example CLI display output for the command.

```
<Broadcom FASTPATH SWITCHING> show hosts

Host name..................... Device
Default domain................ gm.com
Default domain list........... yahoo.com, Stanford.edu,
rediff.com
Domain Name lookup............ Enabled
Number of retries............. 5
Retry timeout period.......... 1500
Name servers (Preference order)... 176.16.1.18 176.16.1.19
DNS Client Source Interface..... (not configured)

Configured host name-to-address mapping:

Host                          Addresses
----------------------------- -----------------------------
accounting.gm.com             176.16.8.8

Host       Total  ElapsedTypeAddresses
-------------- -------- ------    --------     --------------
www.stanford.edu   72    3        IP 171.64.14.203
```

IP Address Conflict Commands

The commands in this section help troubleshoot IP address conflicts.

ip address-conflict-detect run

This command triggers the switch to run active address conflict detection by sending gratuitous ARP packets for IPv4 addresses on the switch.

Format	`ip address-conflict-detect run`
Mode	◆ Global Config ◆ Virtual Router Config

show ip address-conflict

This command displays the status information corresponding to the last detected address conflict.

Format	`show ip address-conflict`
Modes	Privileged EXEC

Term	Definition
Address Conflict Detection Status	Identifies whether the switch has detected an address conflict on any IP address.
Last Conflicting IP Address	The IP Address that was last detected as conflicting on any interface.
Last Conflicting MAC Address	The MAC Address of the conflicting host that was last detected on any interface.
Time Since Conflict Detected	The time in days, hours, minutes and seconds since the last address conflict was detected.

clear ip address-conflict-detect

This command clears the detected address conflict status information for the specified virtual router. If no router is specified, the command is executed for the default router.

Format	`clear ip address-conflict-detect [vrf` *`vrf-name`*`]`
Modes	Privileged EXEC

Serviceability Packet Tracing Commands

These commands improve the capability of network engineers to diagnose conditions affecting their FASTPATH product.

CAUTION
The output of “debug” commands can be long and may adversely affect system performance.

capture start

Use the command **capture start** to manually start capturing CPU packets for packet trace.

The packet capture operates in three modes:

- capture file
- remote capture
- capture line

The command is not persistent across a reboot cycle.

Format	`capture start [{all|receive|transmit}]`
Mode	Privileged EXEC

Parameter	Description
all	Capture all traffic.
receive	Capture only received traffic.
transmit	Capture only transmitted traffic.

capture stop

Use the command **capture stop** to manually stop capturing CPU packets for packet trace.

Format	`capture stop`
Mode	Privileged EXEC

capture file|remote|line

Use this command to configure file capture options. The command is persistent across a reboot cycle.

Format	`capture {file|remote|line}`
Mode	Global Config

Parameter	Description
file	In the capture file mode, the captured packets are stored in a file on NVRAM. The maximum file size defaults to 524288 bytes. The switch can transfer the file to a TFTP server via TFTP, SFTP, SCP via CLI, and SNMP. The file is formatted in pcap format, is named cpuPktCapture.pcap, and can be examined using network analyzer tools such as Wireshark or Ethereal. Starting a file capture automatically terminates any remote capture sessions and line capturing. After the packet capture is activated, the capture proceeds until the capture file reaches its maximum size, or until the capture is stopped manually using the CLI command **capture stop**.

Parameter	Description
remote	In the remote capture mode, the captured packets are redirected in real time to an external PC running the Wireshark tool for Microsoft Windows. A packet capture server runs on the switch side and sends the captured packets via a TCP connection to the Wireshark tool. The remote capture can be enabled or disabled using the CLI. There should be a Windows PC with the Wireshark tool to display the captured file. When using the remote capture mode, the switch does not store any captured data locally on its file system. You can configure the IP port number for connecting Wireshark to the switch. The default port number is 2002. If a firewall is installed between the Wireshark PC and the switch, then these ports must be allowed to pass through the firewall. You must configure the firewall to allow the Wireshark PC to initiate TCP connections to the switch. If the client successfully connects to the switch, the CPU packets are sent to the client PC, then Wireshark receives the packets and displays them. This continues until the session is terminated by either end. Starting a remote capture session automatically terminates the file capture and line capturing.
line	In the capture line mode, the captured packets are saved into the RAM and can be displayed on the CLI. Starting a line capture automatically terminates any remote capture session and capturing into a file. There is a maximum 128 packets of maximum 128 bytes that can be captured and displayed in line mode.

capture remote port

Use this command to configure file capture options. The command is persistent across a reboot cycle. The *id* parameter is a TCP port number from 1024–49151.

Format	`capture remote port` *id*
Mode	Global Config

capture file size

Use this command to configure file capture options. The command is persistent across a reboot cycle. The *max-file-size* parameter is the maximum size the pcap file can reach, which is 2–512 KB.

Format	`capture file size` *max file size*
Mode	Global Config

capture line wrap

This command enables wrapping of captured packets in line mode when the captured packets reaches full capacity.

Format	`capture line wrap`
Mode	Global Config

no capture line wrap

This command disables wrapping of captured packets and configures capture packet to stop when the captured packet capacity is full.

Format	`no capture line wrap`
Mode	Global Config

show capture packets

Use this command to display packets captured and saved to RAM. It is possible to capture and save into RAM, packets that are received or transmitted through the CPU. A maximum 128 packets can be saved into RAM per capturing session. A maximum 128 bytes per packet can be saved into the RAM. If a packet holds more than 128 bytes, only the first 128 bytes are saved; data more than 128 bytes is skipped and cannot be displayed in the CLI.

Capturing packets is stopped automatically when 128 packets are captured and have not yet been displayed during a capture session. Captured packets are not retained after a reload cycle.

Format	`show capture packets`
Mode	Privileged EXEC

debug aaa accounting

This command is useful to debug accounting configuration and functionality in User Manager.

Format	`debug aaa accounting`
Mode	Privileged EXEC

no debug aaa accounting

Use this command to turn off debugging of User Manager accounting functionality.

Format	`no debug aaa accounting`
Mode	Privileged EXEC

debug aaa authorization

Use this command to enable the tracing for AAA in User Manager. This is useful to debug authorization configuration and functionality in the User Manager. Each of the parameters are used to configure authorization debug flags.

Format	`debug aaa authorization commands|exec`
Mode	Privileged EXEC

no debug aaa authorization

Use this command to turn off debugging of the User Manager authorization functionality.

Format	`no debug aaa authorization`
Mode	Privileged EXEC

The following is an example of the command.

```
(Switching) #debug aaa authorization
Tacacs authorization receive packet tracing enabled.

(Switching) #debug tacacs authorization packet transmit

authorization tracing enabled.

(Switching) #no debug aaa authorization

AAA authorization tracing enabled

(Switching) #
```

debug authentication

This command displays either the debug trace for either a single event or all events for an interface

Default	none
Format	`debug authentication packet {all | event}` *`interface`*
Mode	Privileged EXEC

debug clear

This command disables all previously enabled “debug” traces.

Default	disabled
Format	`debug clear`
Mode	Privileged EXEC

debug console

This command enables the display of “debug” trace output on the login session in which it is executed. Debug console display must be enabled in order to view any trace output. The output of debug trace commands will appear on all login sessions for which debug console has been enabled. The configuration of this command remains in effect for the life of the login session. The effect of this command is not persistent across resets.

Default	disabled

Format	`debug console`
Mode	Privileged EXEC

no debug console

This command disables the display of “debug” trace output on the login session in which it is executed.

Format	`no debug console`
Mode	Privileged EXEC

debug crashlog

Use this command to view information contained in the crash log file that the system maintains when it experiences an unexpected reset. The crash log file contains the following information:

- Log Status
- Buffered logging
- Event logging
- Persistent logging
- System Information (output of sysapiMbufDump)
- Message Queue Debug Information
- Memory Debug Information
- Memory Debug Status
- OS Information (output of osapiShowTasks)
- /proc information (meminfo, cpuinfo, interrupts, version and net/sockstat)

Default	disabled
Format	`debug crashlog {[kernel] crashlog-number [upload url] | proc | verbose | deleteall}`
Mode	Privileged EXEC

Parameter	Description
kernel	View the crash log file for the kernel

Parameter	Description
crashlog-number	Specifies the file number to view. The system maintains up to four copies, and the valid range is 1–4."deb
upload *url*	To upload the crash log (or crash dump) to a TFTP server, use the `upload` keyword and specify the required TFTP server information.
proc	View the application process crashlog.
verbose	Enable the verbose crashlog.
deleteall	Delete all crash log files on the system.
data	Crash log data recorder.
crashdump-number	Specifies the crash dump number to view. The valid range is 0–2.
download *url*	To download a crash dump to the switch, use the `download` keyword and specify the required TFTP server information.
component-id	The ID of the component that caused the crash.
item-number	The item number.
additional-parameter	Additional parameters to include.

debug debug-config

Use this command to download or upload the debug-config.ini file. The debug-config. ini file executes CLI commands (including devshell and drivshell commands) on specific predefined events. The debug config file is created manually and downloaded to the switch.

Default	disabled
Format	`debug debug-config {download <url> | upload <url>}`
Mode	Privileged EXEC

debug dhcp packet

This command displays “debug” information about DHCPv4 client activities and traces DHCPv4 packets to and from the local DHCPv4 client.

Default	disabled
Format	`debug dhcp packet [transmit | receive]`
Mode	Privileged EXEC

no debug dhcp

This command disables the display of “debug” trace output for DHCPv4 client activity.

Format	`no debug dhcp packet [transmit | receive]`
Mode	Privileged EXEC

debug dot1x packet

Use this command to enable dot1x packet debug trace.

Default	disabled
Format	`debug dot1x`
Mode	Privileged EXEC

no debug dot1x packet

Use this command to disable dot1x packet debug trace.

Format	`no debug dot1x`
Mode	Privileged EXEC

debug igmpsnooping packet

This command enables tracing of IGMP Snooping packets received and transmitted by the switch.

Default	disabled
Format	`debug igmpsnooping packet`

Mode	Privileged EXEC

no debug igmpsnooping packet

This command disables tracing of IGMP Snooping packets.

Format	`no debug igmpsnooping packet`
Mode	Privileged EXEC

debug igmpsnooping packet transmit

This command enables tracing of IGMP Snooping packets transmitted by the switch. Snooping should be enabled on the device and the interface in order to monitor packets for a particular interface.

Default	disabled
Format	`debug igmpsnooping packet transmit`
Mode	Privileged EXEC

A sample output of the trace message is shown below.

```
<15> JAN 01 02:45:06 192.168.17.29-1 IGMPSNOOP[185429992]:
igmp_snooping_debug.c(116) 908 % Pkt TX - Intf: 1/0/20(20),
Vlan_Id:1 Src_Mac: 00:03:0e:00:00:00 Dest_Mac: 01:00:5e:00:00:01
Src_IP: 9.1.1.1 Dest_IP: 225.0.0.1 Type: V2_Membership_Report
Group: 225.0.0.1
```

The following parameters are displayed in the trace message:

Parameter	Definition
TX	A packet transmitted by the device.
Intf	The interface that the packet went out on. Format used is unit/slot/port (internal interface number). Unit is always shown as 1 for interfaces.
Src_Mac	Source MAC address of the packet.
Dest_Mac	Destination multicast MAC address of the packet.
Src_IP	The source IP address in the IP header in the packet.

Parameter	Definition
Dest_IP	The destination multicast IP address in the packet.
Type	The type of IGMP packet. Type can be one of the following: ◆ `Membership Query` – IGMP Membership Query ◆ `V1_Membership_Report` – IGMP Version 1 Membership Report ◆ `V2_Membership_Report` – IGMP Version 2 Membership Report ◆ `V3_Membership_Report` – IGMP Version 3 Membership Report ◆ `V2_Leave_Group` – IGMP Version 2 Leave Group
Group	Multicast group address in the IGMP header.

no debug igmpsnooping transmit

This command disables tracing of transmitted IGMP snooping packets.

Format	`no debug igmpsnooping transmit`
Mode	Privileged EXEC

debug igmpsnooping packet receive

This command enables tracing of IGMP Snooping packets received by the switch. Snooping should be enabled on the device and the interface in order to monitor packets for a particular interface.

Default	disabled
Format	`debug igmpsnooping packet receive`
Mode	Privileged EXEC

A sample output of the trace message is shown below.

```
<15> JAN 01 02:45:06 192.168.17.29-1 IGMPSNOOP[185429992]:
igmp_snooping_debug.c(116) 908 % Pkt RX - Intf: 1/0/20(20),
Vlan_Id:1 Src_Mac: 00:03:0e:00:00:10 Dest_Mac: 01:00:5e:00:00:05
```

```
Src_IP: 11.1.1.1 Dest_IP: 225.0.0.5 Type: Membership_Query Group:
225.0.0.5
```

The following parameters are displayed in the trace message:

Parameter	Definition
RX	A packet received by the device.
Intf	The interface that the packet went out on. Format used is unit/slot/port (internal interface number). Unit is always shown as 1 for interfaces.
Src_Mac	Source MAC address of the packet.
Dest_Mac	Destination multicast MAC address of the packet.
Src_IP	The source IP address in the ip header in the packet.
Dest_IP	The destination multicast ip address in the packet.
Type	The type of IGMP packet. Type can be one of the following: ◆ `Membership_Query` – IGMP Membership Query ◆ `V1_Membership_Report` – IGMP Version 1 Membership Report ◆ `V2_Membership_Report` – IGMP Version 2 Membership Report ◆ `V3_Membership_Report` – IGMP Version 3 Membership Report ◆ `V2_Leave_Group` – IGMP Version 2 Leave Group
Group	Multicast group address in the IGMP header.

no debug igmpsnooping receive

This command disables tracing of received IGMP Snooping packets.

Format	`no debug igmpsnooping receive`
Mode	Privileged EXEC

debug ipv6 dhcp

This command displays “debug” information about DHCPv6 client activities and traces DHCPv6 packets to and from the local DHCPv6 client.

Default	disabled
Format	`debug ipv6 dhcp`
Mode	Privileged EXEC

no debug ipv6 dhcp

This command disables the display of “debug” trace output for DHCPv6 client activity.

Format	`no debug ipv6 dhcp`
Mode	Privileged EXEC

debug lacp packet

This command enables tracing of LACP packets received and transmitted by the switch.

Default	disabled
Format	`debug lacp packet`
Mode	Privileged EXEC

A sample output of the trace message is shown below.

```
<15> JAN 01 14:04:51 10.254.24.31-1 DOT3AD[183697744]:
dot3ad_debug.c(385) 58 %%
 Pkt TX - Intf: 1/0/1(1), Type: LACP, Sys: 00:11:88:14:62:e1,
State: 0x47, Key:
0x36
```

no debug lacp packet

This command disables tracing of LACP packets.

Format	`no debug lacp packet`
Mode	Privileged EXEC

debug mldsnooping packet

Use this command to trace MLD snooping packet reception and transmission. **receive** traces only received MLD snooping packets and **transmit** traces only transmitted MLD snooping packets. When neither keyword is used in the command, then all MLD snooping packet traces are dumped. Vital information such as source address, destination address, control packet type, packet length, and the interface on which the packet is received or transmitted is displayed on the console.

Default	disabled
Format	`debug mldsnooping packet [receive | transmit]`
Mode	Privileged EXEC

no debug mldsnooping packet

Use this command to disable debug tracing of MLD snooping packet reception and transmission.

debug ping packet

This command enables tracing of ICMP echo requests and responses. The command traces pings on the network port/ service port for switching packages. For routing packages, pings are traced on the routing ports as well. If specified, pings can be traced on the virtual router.

Default	disabled
Format	`debug ping packet [vrf vrf-name]`
Mode	Privileged EXEC

A sample output of the trace message is shown below.

```
<15> JAN 01 00:21:22 192.168.17.29-1 SIM[181040176]:
sim_debug.c(128) 20 % Pkt TX - Intf: 1/0/1(1),
SRC_IP:10.50.50.2, DEST_IP:10.50.50.1, Type:ECHO_REQUEST


<15> JAN 01 00:21:22 192.168.17.29-1 SIM[182813968]:
sim_debug.c(82) 21 % Pkt RX - Intf: 1/0/1(1), S
RC_IP:10.50.50.1, DEST_IP:10.50.50.2, Type:ECHO_REPLY
```

The following parameters are displayed in the trace message:

Parameter	Definition
TX/RX	TX refers to a packet transmitted by the device. RX refers to packets received by the device.
Intf	The interface that the packet came in or went out on. Format used is unit/slot/port (internal interface number). Unit is always shown as 1.
SRC_IP	The source IP address in the IP header in the packet.
DEST_IP	The destination IP address in the IP header in the packet.
Type	Type determines whether or not the ICMP message is a REQUEST or a RESPONSE.

no debug ping packet

This command disables tracing of ICMP echo requests and responses.

Format	`no debug ping packet`
Mode	Privileged EXEC

debug sflow packet

Use this command to enable sFlow debug packet trace.

Default	disabled
Format	`debug sflow packet`
Mode	Privileged EXEC

no debug sflow packet

Use this command to disable sFlow debug packet trace.

Format	`no debug sflow packet`
Mode	Privileged EXEC

debug spanning-tree bpdu

This command enables tracing of spanning tree BPDUs received and transmitted by the switch.

Default	disabled
Format	`debug spanning-tree bpdu`
Mode	Privileged EXEC

no debug spanning-tree bpdu

This command disables tracing of spanning tree BPDUs.

Format	`no debug spanning-tree bpdu`
Mode	Privileged EXEC

debug spanning-tree bpdu receive

This command enables tracing of spanning tree BPDUs received by the switch. Spanning tree should be enabled on the device and on the interface in order to monitor packets for a particular interface.

Default	disabled
Format	`debug spanning-tree bpdu receive`
Mode	Privileged EXEC

A sample output of the trace message is shown below.

```
<15> JAN 01 01:02:04 192.168.17.29-1 DOT1S[191096896]:
dot1s_debug.c(1249) 101 % Pkt RX - Intf: 1/0/9(9), Source_Mac:
00:11:88:4e:c2:10 Version: 3, Root Mac: 00:11:88:4e:c2:00, Root
Priority: 0x8000 Path Cost: 0
```

The following parameters are displayed in the trace message:

Parameter	Definition
RX	A packet received by the device.
Intf	The interface that the packet came in on. Format used is unit/port/slot (internal interface number). Unit is always shown as 1 for interfaces on a non-stacking device.

Parameter	Definition
Source_Mac	Source MAC address of the packet.
Version	Spanning tree protocol version (0-3). 0 refers to STP, 2 RSTP and 3 MSTP.
Root_Mac	MAC address of the CIST root bridge.
Root_Priority	Priority of the CIST root bridge. The value is between 0 and 61440. It is displayed in hex in multiples of 4096.
Path_Cost	External root path cost component of the BPDU.

no debug spanning-tree bpdu receive

This command disables tracing of received spanning tree BPDUs.

Format	`no debug spanning-tree bpdu receive`
Mode	Privileged EXEC

debug spanning-tree bpdu transmit

This command enables tracing of spanning tree BPDUs transmitted by the switch. Spanning tree should be enabled on the device and on the interface in order to monitor packets on a particular interface.

Default	disabled
Format	`debug spanning-tree bpdu transmit`
Mode	Privileged EXEC

A sample output of the trace message is shown below.

```
<15> JAN 01 01:02:04 192.168.17.29-1 DOT1S[191096896]:
dot1s_debug.c(1249) 101 % Pkt TX - Intf: 1/0/7(7), Source_Mac:
00:11:88:4e:c2:00 Version: 3, Root_Mac: 00:11:88:4e:c2:00,
Root_Priority: 0x8000 Path_Cost: 0
```

The following parameters are displayed in the trace message:

Parameter	Definition
TX	A packet transmitted by the device.
Intf	The interface that the packet went out on. Format used is unit/port/slot (internal interface number). Unit is always shown as 1 for interfaces on a non-stacking device.
Source_Mac	Source MAC address of the packet.
Version	Spanning tree protocol version (0-3). 0 refers to STP, 2 RSTP and 3 MSTP.
Root_Mac	MAC address of the CIST root bridge.
Root_Priority	Priority of the CIST root bridge. The value is between 0 and 61440. It is displayed in hex in multiples of 4096.
Path_Cost	External root path cost component of the BPDU.

no debug spanning-tree bpdu transmit

This command disables tracing of transmitted spanning tree BPDUs.

Format	`no debug spanning-tree bpdu transmit`
Mode	Privileged EXEC

debug tacacs

Use the *`debug tacacs packet`* command to turn on TACACS+ debugging.

Format	`debug tacacs {packet [receive | transmit] | accounting | authentication}`
Mode	Global Config

Parameter	Description
packet receive	Turn on TACACS+ receive packet debugs.

Parameter	Description
packet transmit	Turn on TACACS+ transmit packet debugs.
accounting	Turn on TACACS+ authentication debugging.
authentication	Turn on TACACS+ authorization debugging.

debug transfer

This command enables debugging for file transfers.

Format	`debug transfer`
Mode	Privileged EXEC

no debug transfer

This command disables debugging for file transfers.

Format	`no debug transfer`
Mode	Privileged EXEC

show debugging

Use the *`show debugging`* command to display enabled packet tracing configurations.

Format	`show debugging`
Mode	Privileged EXEC

The following shows example CLI display output for the command.

```
console# debug arp
Arp packet tracing enabled.

console# show debugging
Arp packet tracing enabled.
```

no show debugging

Use the *`no show debugging`* command to disable packet tracing configurations.

Format	`no show debugging`

Mode	Privileged EXEC

exception protocol

Use this command to specify the protocol used to store the core dump file.

Default	None
Format	`exception protocol {nfs | tftp | ftp | local | usb | none}`
Mode	Global Config

no exception protocol

Use this command to reset the exception protocol configuration to its factory default value.

Default	None
Format	`no exception protocol`
Mode	Global Config

exception dump tftp-server

Use this command to configure the IP address of a remote TFTP server in order to dump core files to an external server.

Default	None
Format	`exception dump tftp-server {`*`ip-address`*`}`
Mode	Global Config

no exception dump tftp-server

Use this command to reset the exception dump remote server configuration to its factory default value.

Default	None
Format	`no exception dump tftp-server`
Mode	Global Config

exception dump nfs

Use this command to configure an NFS mount point in order to dump core file to the NFS file system.

Default	None
Format	`exception dump nfs` *`ip-address/dir`*
Mode	Global Config

no exception dump nfs

Use this command to reset the exception dump NFS mount point configuration to its factory default value.

Default	None
Format	`no exception dump nfs`
Mode	Global Config

exception dump filepath

Use this command to configure a file-path to dump core file to a TFTP server, NFS mount or USB device subdirectory.

Default	None
Format	`exception dump filepath` *`dir`*
Mode	Global Config

no exception dump filepath

Use this command to reset the exception dump filepath configuration to its factory default value.

Default	None
Format	`exception dump filepath`
Mode	Global Config

exception core-file

Use this command to configure a prefix for a core-file name. The core file name is generated with the prefix as follows:

If *hostname* is selected:
file-name-prefix_hostname_Time_Stamp.bin

If *hostname* is not selected:
file-name-prefix_MAC_Address_Time_Stamp.bin

If *hostname* is configured the core file name takes the *hostname*, otherwise the core-file names uses the MAC address when generating a core dump file. The prefix length is 15 characters.

Default	Core
Format	`exception core-file {`*`file-name-prefix`* `| [hostname] | [time-stamp]}`
Mode	Global Config

no exception core-file

Use this command to reset the exception core file prefix configuration to its factory default value. The hostname and time-stamp are disabled.

Default	Core
Format	`no exception core-file`
Mode	Global Config

exception switch-chip-register

This command enables or disables the switch-chip-register dump in case of an exception. The switch-chip-register dump is taken only for a master unit and not for member units

Default	Disable
Format	`exception switch-chip-register {enable | disable}`
Mode	Global Config

exception dump ftp-server

This command configures the IP address of remote FTP server to dump core files to an external server. If the username and password are not configured, the switch uses anonymous FTP. (The FTP server should be configured to accept anonymous FTP.)

Default	None
Format	`exception dump ftp-server` *`ip-address`* [{`username` *`user-name`* `password` *`password`*}]
Mode	Global Config

no exception dump ftp-server

This command resets exception dump remote FTP server configuration to its factory default value. This command also resets the FTP username and password to empty string.

Default	None
Format	`no exception dump ftp-server`
Mode	Global Config

exception dump compression

This command enables compression mode.

Default	Enabled
Format	`exception dump compression`
Mode	Global Config

no exception dump compression

This command disables compression mode.

Default	None
Format	`no exception compression`
Mode	Global Config

write core

Use the *`write core`* command to generate a core dump file on demand. The *`write core test`* command is helpful when testing the core dump setup. For example, if the TFTP protocol is configured, *`write core test`* communicates

with the TFTP server and informs the user if the TFTP server can be contacted. Similarly, if protocol is configured as *nfs*, this command mounts and unmounts the file system and informs the user of the status.

Note

write core reloads the switch which is useful when the device malfunctions, but has not crashed.

For *write core test*, the destination file name is used for the TFTP test. Optionally, you can specify the destination file name when the protocol is configured as TFTP.

Default	None
Format	`write core [test [dest_file_name]]`
Mode	Privileged EXEC

debug exception

The command displays core dump features support.

Default	None
Format	`debug exception`
Mode	Privileged EXEC

show exception

Use this command to display the configuration parameters for generating a core dump file.

Default	None
Format	`show exception`
Mode	Privileged EXEC

The following shows an example of this command.

```
(CN1610) #show exception

Coredump file name.............................. core
Coredump filename uses hostname................. False
Coredump filename uses time-stamp.............. TRUE
```

```
TFTP server IP.............................
FTP server IP..............................
FTP user name..............................
FTP password...............................
File path..................................... ./.
Protocol..................................... none
Switch-chip-register......................... False
Compression mode............................. TRUE
```

show exception log

This command displays core dump traces on the local file system.

Default	None
Format	`show exception log [previous]`
Mode	Privileged EXEC, Config Mode

logging persistent

Use this command to configure the Persistent logging for the switch. The severity level of logging messages is specified at severity level. Possible values for severity level are (emergency|0, alert|1, critical|2, error|3, warning|4, notice|5, info|6, debug|7).

Default	Disable
Format	`logging persistent` *`severity level`*
Mode	Global Config

no logging persistent

Use this command to disable the persistent logging in the switch.

Format	`no logging persistent`
Mode	Global Config

mbuf

Use this command to configure memory buffer (MBUF) threshold limits and generate notifications when MBUF limits have been reached.

Format	`mbuf {falling-threshold | rising threshold | severity}`

Mode	Global Config

Field	Description
Rising Threshold	The percentage of the memory buffer resources that, when exceeded for the configured rising interval, triggers a notification. The range is 1 to 100. The default is 0 (disabled).
Falling Threshold	The percentage of memory buffer resources that, when usage falls below this level for the configured interval, triggers a notification. The range is 1 to 100. The default is 0 (disabled).
Severity	The severity level at which Mbuf logs messages. The range is 1 to 7. The default is 5 (L7_LOG_SEVERITY_NOTICE).

show mbuf

Use this command to display the memory buffer (MBUF) Utilization Monitoring parameters.

Format	`show mbuf`
Mode	Privileged EXEC

Field	Description
Rising Threshold	The percentage of the memory buffer resources that, when exceeded for the configured rising interval, triggers a notification. The range is 1 to 100. The default is 0 (disabled).
Falling Threshold	The percentage of memory buffer resources that, when usage falls below this level for the configured interval, triggers a notification. The range is 1 to 100. The default is 0 (disabled).
Severity	The severity level.

show mbuf total

Use this command to display memory buffer (MBUF) information.

Format	`show mbuf total`
Mode	Privileged EXEC

Field	Description
Mbufs Total	Total number of message buffers in the system.
Mbufs Free	Number of message buffers currently available.
Mbufs Rx Used	Number of message buffers currently in use.
Total Rx Norm Alloc Attempts	Number of times the system tried to allocate a message buffer allocation of class RX Norm.
Total Rx Mid2 Alloc Attempts	Number of times the system tried to allocate a message buffer allocation of class RX Mid2.
Total Rx Mid1 Alloc Attempts	Number of times the system tried to allocate a message buffer allocation of class RX Mid1.
Total Rx Mid0 Alloc Attempts	Number of times the system tried to allocate a message buffer allocation of class RX Mid0.
Total Rx High Alloc Attempts	Number of times the system tried to allocate a message buffer allocation of class RX High.
Total Tx Alloc Attempts	Number of times the system tried to allocate a message buffer allocation of class TX.
Total Rx Norm Alloc Failures	Number of message buffer allocation failures for RX Norm class of message buffer.
Total Rx Mid2 Alloc Failures	Number of message buffer allocation failures for RX Mid2 class of message buffer.
Total Rx Mid1 Alloc Failures	Number of message buffer allocation failures for RX Mid1 class of message buffer.
Total Rx Mid0 Alloc Failures	Number of message buffer allocation failures for RX Mid0 class of message buffer.

Field	Description
Total Rx High Alloc Failures	Number of message buffer allocation failures for RX High class of message buffer.
Total Tx Alloc Failures	Number of message buffer allocation failures for TX class of message buffer.

show msg-queue

Use this command to display the message queues.

Default	None
Format	`show msg-queue`
Mode	Privileged EXEC mode

Support Mode Commands

Support mode is hidden and available when the *techsupport enable* command is executed. techsupport mode is disabled by default. Configurations related to support mode are shown in the *show tech-support* command. They can be persisted by using the command *save* in support mode. Support configurations are stored in a separate binary config file, which cannot be uploaded or downloaded.

techsupport enable

Use this command to allow access to Support mode.

Default	Disabled
Format	techsupport enable
Mode	Privileged EXEC

console

Use this command to enable the display of support debug for this session.

Default	Disabled
Format	console
Mode	Support

save

Use this command to save the trace configuration to non-volatile storage.

Format	save
Mode	Support

snapshot routing

Use this command in Support mode to dump a set of routing debug information to capture the current state of routing on the switch. The output is written to the console and can be extensive.

Format	*snapshot routing*

Mode	Support

snapshot multicast

Use this command in Support mode to dump a set of IP multicast debug information to capture the current state of multicast on the switch. The output is written to the console and can be extensive.

Format	*snapshot multicast*
Mode	Support

snapshot system

Use this command in Support mode to dump a set of system debug information to capture the current state of the device. The output is written to the console and can be extensive.

Format	*snapshot multicast*
Mode	Support

telnetd

Use this command in Support mode to start or stop the Telnet daemon on the switch.

Format	*telnetd {start | stop}*
Mode	Support

BCM Shell Command

The BCM (SDK) shell is mainly used for debugging the Broadcom SDK. BCM shell commands can be executed directly from the CLI without entering the BCM shell itself by using the keyword *drivshell* before the BCM command. However, you can also enter the BCM shell to directly execute any of the BCM commands on the shell using the *bcmsh* command.

bcmsh

The *bcmsh* command is used to enter into the BCM shells from Privileged EXEC mode. Only users with Level 15 permissions can execute this command. Management is blocked during this mode; the user is notified and asked whether to continue. This command is only supported on the serial console and not via telnet/ssh.

Format	*bcmsh*
Mode	Privileged EXEC

Note
To exit the shell and return to the CLI, enter *exit*.

sFlow Commands

sFlow is the standard for monitoring high-speed switched and routed networks. sFlow technology is built into network equipment and gives complete visibility into network activity, enabling effective management and control of network resources.

sflow receiver

Use this command to configure the sFlow collector parameters (owner string, receiver timeout, max datagram size, IP address, and port).

Format	`sflow receiver` *`rcvr_idx`* {`owner` *`owner-string`* `timeout` *`rcvr_timeout`* | `max datagram` *`size`* | `ip` *`ip`* | `port` *`port`*}
Mode	Global Config

Parameter	Description
Receiver Owner	The identity string for the receiver, the entity making use of this sFlowRcvrTable entry. The range is 127 characters. The default is a null string. The empty string indicates that the entry is currently unclaimed and the receiver configuration is reset to the default values. An entity wishing to claim an sFlowRcvrTable entry must ensure that the entry is unclaimed before trying to claim it. The entry is claimed by setting the owner string to a non-null value. The entry must be claimed before assigning a receiver to a sampler or poller.
Receiver Timeout	The time, in seconds, remaining before the sampler or poller is released and stops sending samples to receiver. A management entity wanting to maintain control of the sampler is responsible for setting a new value before the old one expires. The allowed range is 0-2147483647 seconds. The default is zero (0).
No Timeout	The configured entry will be in the config until you explicitly removes the entry.

Parameter	Description
Receiver Max Datagram Size	The maximum number of data bytes that can be sent in a single sample datagram. The management entity should set this value to avoid fragmentation of the sFlow datagrams. The allowed range is 200 to 9116). The default is 1400.
Receiver IP	The sFlow receiver IP address. If set to 0.0.0.0, no sFlow datagrams will be sent. The default is 0.0.0.0.
Receiver Port	The destination Layer4 UDP port for sFlow datagrams. The range is 1-65535. The default is 6343.

no sflow receiver

Use this command to set the sFlow collector parameters back to the defaults.

Format	`no sflow receiver` *`indx`* {`ip` *`ip-address`* | `maxdatagram` *`size`* | `owner` *`string`* `timeout` *`interval`* | `port` *`14-port`*}
Mode	Global Config

sflow receiver owner timeout

Use this command to configure a receiver as a timeout entry. As the sFlow receiver is configured as a timeout entry, information related to sampler and pollers are also shown in the running-config and are retained after reboot.

If a receiver is configured with a specific value, these configurations will not be shown in running-config. Samplers and pollers information related to this receiver will also not be shown in running-config.

Format	`sflow receiver` *`index`* `owner` *`owner-string`* `timeout`
Mode	Global Config

Field	Description
index	Receiver index identifier. The range is 1 to 8.

Field	Description
Receiver Owner	The owner name corresponds to the receiver name. The identity string for the receiver, the entity making use of this sFlowRcvrTable entry. The range is 127 characters. The default is a null string. The empty string indicates that the entry is currently unclaimed and the receiver configuration is reset to the default values. An entity wishing to claim an sFlowRcvrTable entry must ensure that the entry is unclaimed before trying to claim it. The entry is claimed by setting the owner string to a non-null value. The entry must be claimed before assigning a receiver to a sampler or poller.

sflow receiver owner notimeout

Use this command to configure a receiver as a non-timeout entry. Unlike entries configured with a specific timeout value, this command will be shown in show running-config and retained after reboot. As the sFlow receiver is configured as a non-timeout entry, information related to sampler and pollers will also be shown in the running-config and will be retained after reboot.

If a receiver is configured with a specific value, these configurations will not be shown in running-config. Samplers and pollers information related to this receiver will also not be shown in running-config.

Format	`sflow receiver` *`index`* `owner` *`owner-string`* `notimeout`
Mode	Global Config

Field	Description
index	Receiver index identifier. The range is 1 to 8.

Field	Description
Receiver Owner	The owner name corresponds to the receiver name. The identity string for the receiver, the entity making use of this sFlowRcvrTable entry. The range is 127 characters. The default is a null string. The empty string indicates that the entry is currently unclaimed and the receiver configuration is reset to the default values. An entity wishing to claim an sFlowRcvrTable entry must ensure that the entry is unclaimed before trying to claim it. The entry is claimed by setting the owner string to a non-null value. The entry must be claimed before assigning a receiver to a sampler or poller.

sflow sampler

A data source configured to collect flow samples is called a poller. Use this command to configure a new sFlow sampler instance on an interface or range of interfaces for this data source if *rcvr_idx* is valid.

Format	`sflow sampler {`*`rcvr-indx`* `| rate` *`sampling-rate`* `| maxheadersize` *`size`*`}`
Mode	Interface Config

Field	Description
Receiver Index	The sFlow Receiver for this sFlow sampler to which flow samples are to be sent. A value of zero (0) means that no receiver is configured, no packets will be sampled. Only active receivers can be set. If a receiver expires, then all samplers associated with the receiver will also expire. Possible values are 1-8. The default is 0.

Field	Description
Maxheadersize	The maximum number of bytes that should be copied from the sampler packet. The range is 20-256. The default is 128. When set to zero (0), all the sampler parameters are set to their corresponding default value.
Sampling Rate	The statistical sampling rate for packet sampling from this source. A sampling rate of 1 counts all packets. A value of zero (0) disables sampling. A value of N means that out of N incoming packets, 1 packet will be sampled. The range is 1024-65536 and 0. The default is 0.

no sflow sampler

Use this command to reset the sFlow sampler instance to the default settings.

Format	`no sflow sampler {`*`rcvr-indx`* `| rate` *`sampling-rate`* `| maxheadersize` *`size`*`}`
Mode	Interface Config

sflow poller

A data source configured to collect counter samples is called a poller. Use this command to enable a new sFlow poller instance on an interface or range of interfaces for this data source if *`rcvr_idx`* is valid.

Format	`sflow poller {`*`rcvr-indx`* `| interval` *`poll-interval`*`}`
Mode	Interface Config

Field	Description
Receiver Index	Enter the sFlow Receiver associated with the sampler/poller. A value of zero (0) means that no receiver is configured. The range is 1-8. The default is 0.

Field	Description
Poll Interval	Enter the sFlow instance polling interval. A poll interval of zero (0) disables counter sampling. When set to zero (0), all the poller parameters are set to their corresponding default value. The range is 0-86400. The default is 0. A value of N means once in N seconds a counter sample is generated.

no sflow poller

Use this command to reset the sFlow poller instance to the default settings.

Format	`no sflow poller [interval]`
Mode	Interface Config

show sflow agent

The sFlow agent collects time-based sampling of network interface statistics and flow-based samples. These are sent to the configured sFlow receivers. Use this command to display the sFlow agent information.

Format	`show sflow agent`
Mode	Privileged EXEC

Field	Description
sFlow Version	Uniquely identifies the version and implementation of this MIB. The version string must have the following structure: MIB Version; Organization; Software Revision where: ◆ MIB Version: 1.3, the version of this MIB. ◆ Organization: Broadcom Corp. ◆ Revision: 1.0
IP Address	The IP address associated with this agent.

The following shows example CLI display output for the command.

```
(CN1610) #show sflow agent
```

```
sFlow Version.............................. 1.3;Broadcom
Corp;1.0
IP Address................................. 10.131.12.66
```

show sflow pollers

Use this command to display the sFlow polling instances created on the switch. Use "-" for range.

Format	`show sflow pollers`
Mode	Privileged EXEC

Field	Description
Poller Data Source	The sFlowDataSource (slot/port) for this sFlow sampler. This agent will support Physical ports only.
Receiver Index	The sFlowReceiver associated with this sFlow counter poller.
Poller Interval	The number of seconds between successive samples of the counters associated with this data source.

show sflow receivers

Use this command to display configuration information related to the sFlow receivers.

Format	`show sflow receivers [`*index*`]`
Mode	Privileged EXEC

Parameter	Description
Receiver Index	The sFlow Receiver associated with the sampler/poller.
Owner String	The identity string for receiver, the entity making use of this sFlowRcvrTable entry.

Parameter	Description
Time Out	The time (in seconds) remaining before the receiver is released and stops sending samples to sFlow receiver. The **no timeout** value of this parameter means that the sFlow receiver is configured as a non-timeout entry.
Max Datagram Size	The maximum number of bytes that can be sent in a single sFlow datagram.
Port	The destination Layer4 UDP port for sFlow datagrams.
IP Address	The sFlow receiver IP address.
Address Type	The sFlow receiver IP address type. For an IPv4 address, the value is 1 and for an IPv6 address, the value is 2.
Datagram Version	The sFlow protocol version to be used while sending samples to sFlow receiver.

The following shows example CLI display output for the **show sflow receivers** command.

```
(CN1610) #show sflow receivers 1
Receiver Index.............................. 1
Owner String................................ tulasi
Time out.................................... 0
IP Address:................................. 0.0.0.0
Address Type................................ 1
Port........................................ 6343
Datagram Version............................ 5
Maximum Datagram Size....................... 1400
```

The following examples show CLI display output for the command when a receiver is configured as a non-timeout entry.

```
(CN1610) #show sflow receivers

Rcvr Owner                              Timeout    Max Dgram Port  IP
Address
Indx String                                         Size
---- -------------------------------- ---------- --------- ----- --
-------------
```

```
1    tulasi                              No Timeout 1400      6343
0.0.0.0 <= No Timeout string
2                                    0         1400      6343  0.0.0.0
3                                    0         1400      6343  0.0.0.0
4                                    0         1400      6343  0.0.0.0
5                                    0         1400      6343  0.0.0.0
6                                    0         1400      6343  0.0.0.0
7                                    0         1400      6343  0.0.0.0
8                                    0         1400      6343  0.0.0.0
```

```
(CN1610) #show sflow receivers 1

Receiver Index.............................. 1
Owner String................................ tulasi
Time out.................................... No Timeout
<= No Timeout string is added
IP Address:................................. 0.0.0.0
Address Type................................ 1
Port........................................ 6343
Datagram Version............................ 5
Maximum Datagram Size....................... 1400
```

show sflow samplers

Use this command to display the sFlow sampling instances created on the switch.

Format	`show sflow samplers`
Mode	Privileged EXEC

Field	Description
Sampler Data Source	The sFlowDataSource (slot/port) for this sFlow sampler. This agent will support Physical ports only.
Receiver Index	The sFlowReceiver configured for this sFlow sampler.
Packet Sampling Rate	The statistical sampling rate for packet sampling from this source.
Max Header Size	The maximum number of bytes that should be copied from a sampled packet to form a flow sample.

Remote Monitoring Commands

Remote Monitoring (RMON) is a method of collecting a variety of data about network traffic. RMON supports 64-bit counters (RFC 3273) and High Capacity Alarm Table (RFC 3434).

Note

There is no configuration command for ether stats and high capacity ether stats. The data source for ether stats and high capacity ether stats are configured during initialization.

rmon alarm

This command sets the RMON alarm entry in the RMON alarm MIB group.

Format	`rmon alarm` *`alarm number variable sample interval`* `{absolute|delta} rising-threshold` *`value`* `[`*`rising-event-index`*`] falling-threshold` *`value`* `[`*`falling-event-index`*`] [startup {`*`rising`*`|`*`falling`*`|`*`rising-falling`*`}] [owner` *`string`*`]`
Mode	Global Config

Parameter	Description
Alarm Index	An index that uniquely identifies an entry in the alarm table. Each entry defines a diagnostic sample at a particular interval for an object on the device. The range is 1 to 65535.
Alarm Variable	The object identifier of the particular variable to be sampled. Only variables that resolve to an ASN.1 primitive type of integer.
Alarm Interval	The interval in seconds over which the data is sampled and compared with the rising and falling thresholds. The range is 1 to 2147483647. The default is 1.

Parameter	Description
Alarm Absolute Value	The value of the statistic during the last sampling period. This object is a read-only, 32-bit signed value.
Alarm Rising Threshold	The rising threshold for the sample statistics. The range is 2147483648 to 2147483647. The default is 1.
Alarm Rising Event Index	The index of the eventEntry that is used when a rising threshold is crossed. The range is 1 to 65535. The default is 1.
Alarm Falling Threshold	The falling threshold for the sample statistics. The range is 2147483648 to 2147483647. The default is 1.
Alarm Falling Event Index	The index of the eventEntry that is used when a falling threshold is crossed. The range is 1 to 65535. The default is 2.
Alarm Startup Alarm	The alarm that may be sent. Possible values are **rising, falling** or both **rising-falling**. The default is **rising-falling**.
Alarm Owner	The owner string associated with the alarm entry. The default is **monitorAlarm**.

The following shows an example of the command.

```
(CN1610) (Config)# rmon alarm 1 ifInErrors.2 30 absolute rising-
threshold 100 1 falling-threshold 10 2 startup rising owner myOwner
```

no rmon alarm

This command deletes the RMON alarm entry.

Format	`no rmon alarm` *`alarm number`*
Mode	Global Config

The following shows an example of the command.

```
(CN1610) (Config)# no rmon alarm 1
```

rmon hcalarm

This command sets the RMON hcalarm entry in the High Capacity RMON alarm MIB group.

Format	`rmon hcalarm` *`alarm number variable sample interval`* `{absolute|delta} rising-threshold high` *`value`* `low` *`value`* `status {positive|negative} [`*`rising-event-index`*`] falling-threshold high` *`value`* `low` *`value`* `status {positive|negative} [`*`falling-event-index`*`] [startup {`*`rising`*`|`*`falling`*`|`*`rising-falling`*`}] [owner` *`string`*`]`
Mode	Global Config

Parameter	Description
High Capacity Alarm Index	An arbitrary integer index value used to uniquely identify the high capacity alarm entry. The range is 1 to 65535.
High Capacity Alarm Variable	The object identifier of the particular variable to be sampled. Only variables that resolve to an ASN.1 primitive type of integer.
High Capacity Alarm Interval	The interval in seconds over which the data is sampled and compared with the rising and falling thresholds. The range is 1 to 2147483647. The default is 1.
High Capacity Alarm Sample Type	The method of sampling the selected variable and calculating the value to be compared against the thresholds. Possible types are **Absolute Value** or **Delta Value**. The default is **Absolute Value**.
High Capacity Alarm Absolute Value	The absolute value (that is, the unsigned value) of the hcAlarmVariable statistic during the last sampling period. The value during the current sampling period is not made available until the period is complete. This object is a 64-bit unsigned value that is Read-Only.

Parameter	Description
High Capacity Alarm Absolute Alarm Status	This object indicates the validity and sign of the data for the high capacity alarm absolute value object (hcAlarmAbsValueobject). Possible status types are **valueNotAvailable**, **valuePositive**, or **valueNegative**. The default is **valueNotAvailable**.
High Capacity Alarm Startup Alarm	High capacity alarm startup alarm that may be sent. Possible values are **rising**, **falling**, or **rising-falling**. The default is **rising-falling**.
High Capacity Alarm Rising-Threshold Absolute Value Low	The lower 32 bits of the absolute value for threshold for the sampled statistic. The range is 0 to 4294967295. The default is 1.
High Capacity Alarm Rising-Threshold Absolute Value High	The upper 32 bits of the absolute value for threshold for the sampled statistic. The range is 0 to 4294967295. The default is 0.
High Capacity Alarm Rising-Threshold Value Status	This object indicates the sign of the data for the rising threshold, as defined by the objects hcAlarmRisingThresAbsValueLow and hcAlarmRisingThresAbsValueHigh. Possible values are **valueNotAvailable**, **valuePositive**, or **valueNegative**. The default is **valuePositive**.
High Capacity Alarm Falling-Threshold Absolute Value Low	The lower 32 bits of the absolute value for threshold for the sampled statistic. The range is 0 to 4294967295. The default is 1.
High Capacity Alarm Falling-Threshold Absolute Value High	The upper 32 bits of the absolute value for threshold for the sampled statistic. The range is 0 to 4294967295. The default is 0.
High Capacity Alarm Falling-Threshold Value Status	This object indicates the sign of the data for the falling threshold, as defined by the objects hcAlarmFallingThresAbsValueLow and hcAlarmFallingThresAbsValueHigh. Possible values are **valueNotAvailable**, **valuePositive**, or **valueNegative**. The default is **valuePositive**.

Parameter	Description
High Capacity Alarm Rising Event Index	The index of the eventEntry that is used when a rising threshold is crossed. The range is 1 to 65535. The default is 1.
High Capacity Alarm Falling Event Index	The index of the eventEntry that is used when a falling threshold is crossed. The range is 1 to 65535. The default is 2.
High Capacity Alarm Failed Attempts	The number of times the associated hcAlarmVariable instance was polled on behalf of the hcAlarmEntry (while in the active state) and the value was not available. This object is a 32-bit counter value that is read-only.
High Capacity Alarm Owner	The owner string associated with the alarm entry. The default is **monitorHCAlarm**.
High Capacity Alarm Storage Type	The type of non-volatile storage configured for this entry. This object is read-only. The default is **volatile**.

The following shows an example of the command.

```
(CN1610) (Config)# rmon hcalarm 1 ifInOctets.1 30 absolute rising-
threshold high 1 low 100 status positive 1 falling-threshold high 1
low 10 status positive startup rising owner myOwner
```

no rmon hcalarm

This command deletes the rmon hcalarm entry.

Format	`no rmon hcalarm` *`alarm number`*
Mode	Global Config

The following shows an example of the command.

```
(CN1610) (Config)# no rmon hcalarm 1
```

rmon event

This command sets the RMON event entry in the RMON event MIB group.

Format	`rmon event` *`event number`* `[description` *`string`*`|log|owner` *`string`*`|trap` *`community`*`]`
Mode	Global Config

Parameter	Description
Event Index	An index that uniquely identifies an entry in the event table. Each such entry defines one event that is to be generated when the appropriate conditions occur. The range is 1 to 65535.
Event Description	A comment describing the event entry. The default is **alarmEvent**.
Event Type	The type of notification that the probe makes about the event. Possible values are **None**, **Log**, **SNMP Trap**, **Log and SNMP Trap**. The default is **None**.
Event Owner	Owner string associated with the entry. The default is **monitorEvent**.
Event Community	The SNMP community specific by this octet string which is used to send an SNMP trap. The default is **public**.

The following shows an example of the command.

```
(CN1610) (Config)# rmon event 1 log description test
```

no rmon event

This command deletes the rmon event entry.

Format	`no rmon event` *`event number`*
Mode	Global Config

The following shows an example of the command.

```
(CN1610) (Config)# no rmon event 1
```

rmon collection history

This command sets the history control parameters of the RMON historyControl MIB group.

Note

This command is not supported on interface range. Each RMON history control collection entry can be configured on only one interface. If you try to configure on multiple interfaces, DUT displays an error.

Format	`rmon collection history` *`index number`* `[buckets` *`number`*`|interval` *`interval in sec`*`|owner` *`string`*`]`
Mode	`Interface` Config

Parameter	Description
History Control Index	An index that uniquely identifies an entry in the historyControl table. Each such entry defines a set of samples at a particular interval for an interface on the device. The range is 1 to 65535.
History Control Data Source	The source interface for which historical data is collected.
History Control Buckets Requested	The requested number of discrete time intervals over which data is to be saved. The range is 1 to 65535. The default is 50.
History Control Buckets Granted	The number of discrete sampling intervals over which data shall be saved. This object is read-only. The default is 10.
History Control Interval	The interval in seconds over which the data is sampled. The range is 1 to 3600. The default is 1800.
History Control Owner	The owner string associated with the history control entry. The default is monitorHistoryControl.

The following shows an example of the command.

```
(CN1610) (Interface 1/0/1)# rmon collection history 1 buckets 10
interval 30 owner myOwner
```

The following shows an example of the command.

```
(CN1610) (Interface 1/0/1-1/0/10)#rmon collection history 1 buckets
10 interval 30 owner myOwner

Error: 'rmon collection history' is not supported on range of
interfaces.
```

no rmon collection history

This command will delete the history control group entry with the specified index number.

Format	`no rmon collection history` *index number*
Mode	`Interface` Config

The following shows an example of the command.

```
(CN1610) (Interface 1/0/1-1/0/10)# no rmon collection history 1
```

show rmon

This command displays the entries in the RMON alarm table.

Format	`show rmon {alarms | alarm` *alarm-index*`}`
Mode	Privileged EXEC

Parameter	Description
Alarm Index	An index that uniquely identifies an entry in the alarm table. Each entry defines a diagnostic sample at a particular interval for an object on the device. The range is 1 to 65535.
Alarm Variable	The object identifier of the particular variable to be sampled. Only variables that resolve to an ASN.1 primitive type of integer.
Alarm Interval	The interval in seconds over which the data is sampled and compared with the rising and falling thresholds. The range is 1 to 2147483647. The default is 1.

Parameter	Description
Alarm Absolute Value	The value of the statistic during the last sampling period. This object is a read-only, 32-bit signed value.
Alarm Rising Threshold	The rising threshold for the sample statistics. The range is 2147483648 to 2147483647. The default is 1.
Alarm Rising Event Index	The index of the eventEntry that is used when a rising threshold is crossed. The range is 1 to 65535. The default is 1.
Alarm Falling Threshold	The falling threshold for the sample statistics. The range is 2147483648 to 2147483647. The default is 1.
Alarm Falling Event Index	The index of the eventEntry that is used when a falling threshold is crossed. The range is 1 to 65535. The default is 2.
Alarm Startup Alarm	The alarm that may be sent. Possible values are **rising, falling** or both **rising-falling**. The default is **rising-falling**.
Alarm Owner	The owner string associated with the alarm entry. The default is **monitorAlarm**.

The following shows example CLI display output for the command.

```
(CN1610) #show rmon alarms

Index    OID                        Owner
---------------------------------------------
1      alarmInterval.1              MibBrowser
2      alarmInterval.1              MibBrowser
```

The following shows example CLI display output for the command.

```
(CN1610) #show rmon alarm 1

Alarm 1
----------
OID: alarmInterval.1
```

```
Last Sample Value: 1
Interval: 1
Sample Type: absolute
Startup Alarm: rising-falling
Rising Threshold: 1
Falling Threshold: 1
Rising Event: 1
Falling Event: 2
Owner: MibBrowser
```

show rmon collection history

This command displays the entries in the RMON history control table.

Format	`show rmon collection history [interfaces slot/port]`
Mode	Privileged EXEC

Parameter	Description
History Control Index	An index that uniquely identifies an entry in the historyControl table. Each such entry defines a set of samples at a particular interval for an interface on the device. The range is 1 to 65535.
History Control Data Source	The source interface for which historical data is collected.
History Control Buckets Requested	The requested number of discrete time intervals over which data is to be saved. The range is 1 to 65535. The default is 50.
History Control Buckets Granted	The number of discrete sampling intervals over which data shall be saved. This object is read-only. The default is 10.
History Control Interval	The interval in seconds over which the data is sampled. The range is 1 to 3600. The default is 1800.
History Control Owner	The owner string associated with the history control entry. The default is monitorHistoryControl.

The following shows example CLI display output for the command.

```
(CN1610) #show rmon collection history

Index   Interface    Interval   Requested   Granted     Owner
                                 Samples    Samples
-------------------------------------------------------------------
----
1       1/0/1        30         10          10          myowner
2       1/0/1        1800       50          10
monitorHistoryControl
3       1/0/2        30         50          10
monitorHistoryControl
4       1/0/2        1800       50          10
monitorHistoryControl
5       1/0/3        30         50          10
monitorHistoryControl
6       1/0/3        1800       50          10
monitorHistoryControl
7       1/0/4        30         50          10
monitorHistoryControl
8       1/0/4        1800       50          10
monitorHistoryControl
9       1/0/5        30         50          10
monitorHistoryControl
10      1/0/5        1800       50          10
monitorHistoryControl
11      1/0/6        30         50          10
monitorHistoryControl
12      1/0/6        1800       50          10
monitorHistoryControl
13      1/0/7        30         50          10
monitorHistoryControl
14      1/0/7        1800       50          10
monitorHistoryControl
15      1/0/8        30         50          10
monitorHistoryControl
16      1/0/8        1800       50          10
monitorHistoryControl
17      1/0/9        30         50          10
monitorHistoryControl
18      1/0/9        1800       50          10
monitorHistoryControl
19      1/0/10       30         50          10
monitorHistoryControl
--More-- or (q)uit
```

The following shows example CLI display output for the command.

```
(CN1610) #show rmon collection history interfaces 1/0/1

Index   Interface    Interval   Requested   Granted     Owner
                                 Samples    Samples
-------------------------------------------------------------------
----
1       1/0/1        30         10          10          myowner
2       1/0/1        1800       50          10
monitorHistoryControl
```

show rmon events

This command displays the entries in the RMON event table.

Format	`show rmon events`
Mode	Privileged EXEC

Parameter	Description
Event Index	An index that uniquely identifies an entry in the event table. Each such entry defines one event that is to be generated when the appropriate conditions occur. The range is 1 to 65535.
Event Description	A comment describing the event entry. The default is **alarmEvent**.
Event Type	The type of notification that the probe makes about the event. Possible values are **None**, **Log**, **SNMP Trap**, **Log and SNMP Trap**. The default is **None**.
Event Owner	Owner string associated with the entry. The default is **monitorEvent**.
Event Community	The SNMP community specific by this octet string which is used to send an SNMP trap. The default is **public**.
Owner	Event owner. The owner string associated with the entry.
Last time sent	The last time over which a log or a SNMP trap message is generated.

The following shows example CLI display output for the command.

```
(CN1610) # show rmon events

Index  Description       Type      Community   Owner      Last time
sent
-------------------------------------------------------------------
-------------
1      test              log       public      MIB        0 days 0
h:0 m:0 s
```

show rmon history

This command displays the specified entry in the RMON history table.

Format	`show rmon history` *index* {`errors [period` *seconds*`]`|`other [period` *seconds*`]`|`throughput [period` *seconds*`]`}
Mode	Privileged EXEC

Parameter	Description
History Control Index	An index that uniquely identifies an entry in the historyControl table. Each such entry defines a set of samples at a particular interval for an interface on the device. The range is 1 to 65535.
History Control Data Source	The source interface for which historical data is collected.
History Control Buckets Requested	The requested number of discrete time intervals over which data is to be saved. The range is 1 to 65535. The default is 50.
History Control Buckets Granted	The number of discrete sampling intervals over which data shall be saved. This object is read-only. The default is 10.
History Control Interval	The interval in seconds over which the data is sampled. The range is 1 to 3600. The default is 1800.
History Control Owner	The owner string associated with the history control entry. The default is monitorHistoryControl.

Parameter	Description
Maximum Table Size	Maximum number of entries that the history table can hold.
Time	Time at which the sample is collected, displayed as period seconds.
CRC Align	Number of CRC align errors.
Undersize Packets	Total number of undersize packets. Packets are less than 64 octets long (excluding framing bits, including FCS octets).
Oversize Packets	Total number of oversize packets. Packets are longer than 1518 octets (excluding framing bits, including FCS octets).
Fragments	Total number of fragment packets. Packets are not an integral number of octets in length or had a bad Frame Check Sequence (FCS), and are less than 64 octets in length (excluding framing bits, including FCS octets).
Jabbers	Total number of jabber packets. Packets are longer than 1518 octets (excluding framing bits, including FCS octets), and are not an integral number of octets in length or had a bad Frame Check Sequence (FCS).
Octets	Total number of octets received on the interface.
Packets	Total number of packets received (including error packets) on the interface.
Broadcast	Total number of good Broadcast packets received on the interface.
Multicast	Total number of good Multicast packets received on the interface.
Util	Port utilization of the interface associated with the history index specified.
Dropped Collisions	Total number of dropped collisions.

The following shows example CLI display output for the command.

```
(CN1610) #show rmon history 1 errors

Sample set: 1   Owner: myowner
Interface: 1/0/1   Interval: 30
Requested Samples: 10   Granted Samples: 10
Maximum table size: 1758

Time                  CRC Align  Undersize Oversize  Fragments
Jabbers
--------------------- ---------- --------- --------- ---------- ---
----
Jan 01 1970 21:41:43  0          0         0         0          0
Jan 01 1970 21:42:14  0          0         0         0          0
Jan 01 1970 21:42:44  0          0         0         0          0
Jan 01 1970 21:43:14  0          0         0         0          0
Jan 01 1970 21:43:44  0          0         0         0          0
Jan 01 1970 21:44:14  0          0         0         0          0
Jan 01 1970 21:44:45  0          0         0         0          0
Jan 01 1970 21:45:15  0          0         0         0          0
Jan 01 1970 21:45:45  0          0         0         0          0
Jan 01 1970 21:46:15  0          0         0         0          0
```

The following shows example CLI display output for the command.

```
(CN1610) #show rmon history 1 throughput

Sample set: 1   Owner: myowner
Interface: 1/0/1   Interval: 30
Requested Samples: 10   Granted Samples: 10
Maximum table size: 1758

Time                 Octets     Packets   Broadcast Multicast  Util
-------------------- ---------- --------- --------- ---------- ----
----
Jan 01 1970 21:41:43 0          0         0         0          1
Jan 01 1970 21:42:14 0          0         0         0          1
Jan 01 1970 21:42:44 0          0         0         0          1
Jan 01 1970 21:43:14 0          0         0         0          1
Jan 01 1970 21:43:44 0          0         0         0          1
Jan 01 1970 21:44:14 0          0         0         0          1
Jan 01 1970 21:44:45 0          0         0         0          1
Jan 01 1970 21:45:15 0          0         0         0          1
Jan 01 1970 21:45:45 0          0         0         0          1
Jan 01 1970 21:46:15 0          0         0         0          1

(CN1610) #show rmon history 1 other
```

```
Sample set: 1   Owner: myowner
Interface: 1/0/1   Interval: 30
Requested Samples: 10   Granted Samples: 10
Maximum table size: 1758

Time                 Dropped Collisions
-------------------- ------- ----------
Jan 01 1970 21:41:43 0       0
Jan 01 1970 21:42:14 0       0
Jan 01 1970 21:42:44 0       0
Jan 01 1970 21:43:14 0       0
Jan 01 1970 21:43:44 0       0
Jan 01 1970 21:44:14 0       0
Jan 01 1970 21:44:45 0       0
Jan 01 1970 21:45:15 0       0
Jan 01 1970 21:45:45 0       0
Jan 01 1970 21:46:15 0       0
```

show rmon log

This command displays the entries in the RMON log table.

Format	`show rmon log [`*`event-index`*`]`
Mode	Privileged EXEC

Parameter	Description
Maximum table size	Maximum number of entries that the log table can hold.
Event	Event index for which the log is generated.
Description	A comment describing the event entry for which the log is generated.
Time	Time at which the event is generated.

The following shows example CLI display output for the command.

```
(CN1610) #show rmon log

Event   Description                   Time
----------------------------------------------
```

The following shows example CLI display output for the command.

```
(CN1610) #show rmon log 1

Maximum table size: 10

Event   Description                    Time
-----------------------------------------------
```

show rmon statistics interfaces

This command displays the RMON statistics for the given interfaces.

Format	`show rmon statistics interfaces slot/port`
Mode	Privileged EXEC

Parameter	Description
Port	slot/port
Dropped	Total number of dropped events on the interface.
Octets	Total number of octets received on the interface.
Packets	Total number of packets received (including error packets) on the interface.
Broadcast	Total number of good broadcast packets received on the interface.
Multicast	Total number of good multicast packets received on the interface.
CRC Align Errors	Total number of packets received have a length (excluding framing bits, including FCS octets) of between 64 and 1518 octets inclusive.
Collisions	Total number of collisions on the interface.
Undersize Pkts	Total number of undersize packets. Packets are less than 64 octets long (excluding framing bits, including FCS octets).

Parameter	Description
Oversize Pkts	Total number of oversize packets. Packets are longer than 1518 octets (excluding framing bits, including FCS octets).
Fragments	Total number of fragment packets. Packets are not an integral number of octets in length or had a bad Frame Check Sequence (FCS), and are less than 64 octets in length (excluding framing bits, including FCS octets).
Jabbers	Total number of jabber packets. Packets are longer than 1518 octets (excluding framing bits, including FCS octets), and are not an integral number of octets in length or had a bad Frame Check Sequence (FCS).
64 Octets	Total number of packets which are 64 octets in length (excluding framing bits, including FCS octets).
65-127 Octets	Total number of packets which are between 65 and 127 octets in length (excluding framing bits, including FCS octets).
128-255 Octets	Total number of packets which are between 128 and 255 octets in length (excluding framing bits, including FCS octets).
256-511 Octets	Total number of packets which are between 256 and 511 octets in length (excluding framing bits, including FCS octets).
512-1023 Octets	Total number of packets which are between 512 and 1023 octets in length (excluding framing bits, including FCS octets).
1024-1518 Octets	Total number of packets which are between 1024 and 1518 octets in length (excluding framing bits, including FCS octets).
HC Overflow Pkts	Total number of HC overflow packets.

Parameter	Description
HC Overflow Octets	Total number of HC overflow octets.
HC Overflow Pkts 64 Octets	Total number of HC overflow packets which are 64 octets in length
HC Overflow Pkts 65 - 127 Octets	Total number of HC overflow packets which are between 65 and 127 octets in length.
HC Overflow Pkts 128 - 255 Octets	Total number of HC overflow packets which are between 128 and 255 octets in length.
HC Overflow Pkts 256 - 511 Octets	Total number of HC overflow packets which are between 256 and 511 octets in length.
HC Overflow Pkts 512 - 1023 Octets	Total number of HC overflow packets which are between 512 and 1023 octets in length.
HC Overflow Pkts 1024 - 1518 Octets	Total number of HC overflow packets which are between 1024 and 1518 octets in length.

The following shows example CLI display output for the command.

```
(CN1610) # show rmon statistics interfaces 1/0/1
Port: 1/0/1
Dropped: 0
Octets: 0  Packets: 0
Broadcast: 0  Multicast: 0
CRC Align Errors: 0  Collisions: 0
Undersize Pkts: 0  Oversize Pkts: 0
Fragments: 0  Jabbers: 0
64 Octets: 0  65 - 127 Octets: 0
128 - 255 Octets: 0  256 - 511 Octets: 0
512 - 1023 Octets: 0  1024 - 1518 Octets: 0
HC Overflow Pkts: 0  HC Pkts: 0
HC Overflow Octets: 0  HC Octets: 0
HC Overflow Pkts 64 Octets: 0  HC Pkts 64 Octets: 0
HC Overflow Pkts 65 - 127 Octets: 0  HC Pkts 65 - 127 Octets: 0
HC Overflow Pkts 128 - 255 Octets: 0  HC Pkts 128 - 255 Octets: 0
HC Overflow Pkts 256 - 511 Octets: 0  HC Pkts 256 - 511 Octets: 0
HC Overflow Pkts 512 - 1023 Octets: 0  HC Pkts 512 - 1023 Octets: 0
HC Overflow Pkts 1024 - 1518 Octets: 0  HC Pkts 1024 - 1518 Octets:
0
```

show rmon hcalarms

This command displays the entries in the RMON high-capacity alarm table.

Format	`show rmon {hcalarms|hcalarm` *`alarm index`*`}`
Mode	Privileged EXEC

Parameter	Description
High Capacity Alarm Index	An arbitrary integer index value used to uniquely identify the high capacity alarm entry. The range is 1 to 65535.
High Capacity Alarm Variable	The object identifier of the particular variable to be sampled. Only variables that resolve to an ASN.1 primitive type of integer.
High Capacity Alarm Interval	The interval in seconds over which the data is sampled and compared with the rising and falling thresholds. The range is 1 to 2147483647. The default is 1.
High Capacity Alarm Sample Type	The method of sampling the selected variable and calculating the value to be compared against the thresholds. Possible types are **Absolute Value** or **Delta Value**. The default is **Absolute Value**.
High Capacity Alarm Absolute Value	The absolute value (that is, the unsigned value) of the hcAlarmVariable statistic during the last sampling period. The value during the current sampling period is not made available until the period is complete. This object is a 64-bit unsigned value that is Read-Only.
High Capacity Alarm Absolute Alarm Status	This object indicates the validity and sign of the data for the high capacity alarm absolute value object (hcAlarmAbsValueobject). Possible status types are **valueNotAvailable**, **valuePositive**, or **valueNegative**. The default is **valueNotAvailable**.
High Capacity Alarm Startup Alarm	High capacity alarm startup alarm that may be sent. Possible values are **rising**, **falling**, or **rising-falling**. The default is **rising-falling**.

Parameter	Description
High Capacity Alarm Rising-Threshold Absolute Value Low	The lower 32 bits of the absolute value for threshold for the sampled statistic. The range is 0 to 4294967295. The default is 1.
High Capacity Alarm Rising-Threshold Absolute Value High	The upper 32 bits of the absolute value for threshold for the sampled statistic. The range is 0 to 4294967295. The default is 0.
High Capacity Alarm Rising-Threshold Value Status	This object indicates the sign of the data for the rising threshold, as defined by the objects hcAlarmRisingThresAbsValueLow and hcAlarmRisingThresAbsValueHigh. Possible values are **valueNotAvailable**, **valuePositive**, or **valueNegative**. The default is **valuePositive**.
High Capacity Alarm Falling-Threshold Absolute Value Low	The lower 32 bits of the absolute value for threshold for the sampled statistic. The range is 0 to 4294967295. The default is 1.
High Capacity Alarm Falling-Threshold Absolute Value High	The upper 32 bits of the absolute value for threshold for the sampled statistic. The range is 0 to 4294967295. The default is 0.
High Capacity Alarm Falling-Threshold Value Status	This object indicates the sign of the data for the falling threshold, as defined by the objects hcAlarmFallingThresAbsValueLow and hcAlarmFallingThresAbsValueHigh. Possible values are **valueNotAvailable**, **valuePositive**, or **valueNegative**. The default is **valuePositive**.
High Capacity Alarm Rising Event Index	The index of the eventEntry that is used when a rising threshold is crossed. The range is 1 to 65535. The default is 1.
High Capacity Alarm Falling Event Index	The index of the eventEntry that is used when a falling threshold is crossed. The range is 1 to 65535. The default is 2.

Parameter	Description
High Capacity Alarm Failed Attempts	The number of times the associated hcAlarmVariable instance was polled on behalf of thie hcAlarmEntry (while in the active state) and the value was not available. This object is a 32-bit counter value that is read-only.
High Capacity Alarm Owner	The owner string associated with the alarm entry. The default is **monitorHCAlarm**.
High Capacity Alarm Storage Type	The type of non-volatile storage configured for this entry. This object is read-only. The default is **volatile**.

The following shows example CLI display output for the command.

```
(CN1610) #show rmon hcalarms

Index    OID                        Owner
-----------------------------------------------
1      alarmInterval.1              MibBrowser
2      alarmInterval.1              MibBrowser

(CN1610) #show rmon hcalarm 1

Alarm 1
----------
OID: alarmInterval.1
Last Sample Value: 1
Interval: 1
Sample Type: absolute
Startup Alarm: rising-falling
Rising Threshold High: 0
Rising Threshold Low: 1
Rising Threshold Status: Positive
Falling Threshold High: 0
Falling Threshold Low: 1
Falling Threshold Status: Positive
Rising Event: 1
Falling Event: 2
Startup Alarm: Rising-Falling
Owner: MibBrowser
```

Switching Commands 5

This chapter describes the switching commands available in the FASTPATH CLI.

The Switching Commands chapter includes the following sections:

Note

The commands in this chapter are in one of three functional groups:

- Show commands display switch settings, statistics, and other information.
- Configuration commands configure features and options of the switch. For every configuration command, there is a show command that displays the configuration setting.
- Clear commands clear some or all of the settings to factory defaults.

Port Configuration Commands

This section describes the commands you use to view and configure port settings.

interface

This command gives you access to the Interface Config mode, which allows you to enable or modify the operation of an interface (port). You can also specify a range of ports to configure at the same time by specifying the starting slot/port and ending slot/port, separated by a hyphen.

Format	`interface {slot/port | slot/port`*`(startrange)`*`-slot/port`*`(endrange)`*`}`
Mode	Global Config

The following example enters Interface Config mode for port 1/0/1:

```
(CN1610) #configure
(CN1610) (config)#interface 1/0/1
(CN1610) (interface 1/0/1)#
```

The following example enters Interface Config mode for ports 1/0/1 through 1/0/4:

```
(CN1610) #configure
(CN1610) (config)#interface 1/0/1-1/0/4
(CN1610) (interface 1/0/1-1/0/4)#
```

auto-negotiate

This command enables automatic negotiation on a port or range of ports.

Default	enabled
Format	`auto-negotiate`
Mode	Interface Config

no auto-negotiate

This command disables automatic negotiation on a port.

Note

Automatic sensing is disabled when automatic negotiation is disabled.

Format	`no auto-negotiate`
Mode	Interface Config

auto-negotiate all

This command enables automatic negotiation on all ports.

Default	enabled
Format	`auto-negotiate all`
Mode	Global Config

no auto-negotiate all

This command disables automatic negotiation on all ports.

Format	`no auto-negotiate all`
Mode	Global Config

description

Use this command to create an alpha-numeric description of an interface or range of interfaces.

Format	`description` *`description`*
Mode	Interface Config

mtu

Use the `mtu` command to set the maximum transmission unit (MTU) size, in bytes, for frames that ingress or egress the interface. You can use the `mtu` command to configure jumbo frame support for physical and port-channel (LAG) interfaces. For the standard FASTPATH implementation, the MTU size is a valid integer between 1522–9216 for tagged packets and a valid integer between 1518 - 9216 for untagged packets.

Note

To receive and process packets, the Ethernet MTU must include any extra bytes that Layer-2 headers might require. To configure the IP MTU size, which is the maximum size of the IP packet (IP Header + IP payload).

Default	1518 (untagged)
Format	`mtu` *`1518-12288`*
Mode	Interface Config

no mtu

This command sets the default MTU size (in bytes) for the interface.

Format	`no mtu`
Mode	Interface Config

shutdown

This command disables a port or range of ports.

Note

You can use the `shutdown` command on physical and port-channel (LAG) interfaces, but not on VLAN routing interfaces.

Default	enabled
Format	`shutdown`
Mode	Interface Config

no shutdown

This command enables a port.

Format	`no shutdown`
Mode	Interface Config

shutdown all

This command disables all ports.

Note

You can use the `shutdown all` command on physical and port-channel (LAG) interfaces, but not on VLAN routing interfaces.

Default	enabled
Format	`shutdown all`
Mode	Global Config

no shutdown all

This command enables all ports.

Format	`no shutdown all`
Mode	Global Config

speed

Use this command to enable or disable auto-negotiation and set the speed that will be advertised by that port. The duplex parameter allows you to set the advertised speed for both half as well as full duplex mode.

Use the `auto` keyword to enable auto-negotiation on the port. Use the command without the `auto` keyword to ensure auto-negotiation is disabled and to set the port speed and mode according to the command values. If auto-negotiation is disabled, the speed and duplex mode must be set.

Default	Auto-negotiation is enabled.
Format	`speed {auto {40G | 10G | 1000 | 100 | 10} [40G | 10G | 1000 | 100 | 10] [half-duplex | full-duplex] | {40G | 10G | 1000 | 100 | 10} {half-duplex | full-duplex}}`
Mode	Interface Config

speed all

This command sets the speed and duplex setting for all interfaces.

Format	`speed all {100 | 10} {half-duplex | full-duplex}`
Mode	Global Config

show port

This command displays port information.

Format	`show port {intf-range | all}`
Mode	Privileged EXEC

Parameter	Definition
Interface	slot/port
Type	If not blank, this field indicates that this port is a special type of port. The possible values are: ◆ **Mirror** — this port is a monitoring port. For more information, see "Port Mirroring Commands" on page 466. ◆ **PC Mbr**— this port is a member of a port-channel (LAG). ◆ **Probe** — this port is a probe port.
Admin Mode	The Port control administration state. The port must be enabled in order for it to be allowed into the network. May be enabled or disabled. The factory default is enabled.
Physical Mode	The desired port speed and duplex mode. If auto-negotiation support is selected, then the duplex mode and speed is set from the auto-negotiation process. Note that the maximum capability of the port (full duplex -100M) is advertised. Otherwise, this object determines the port's duplex mode and transmission rate. The factory default is Auto.
Physical Status	The port speed and duplex mode.
Link Status	The Link is up or down.
Link Trap	This object determines whether or not to send a trap when link status changes. The factory default is enabled.
LACP Mode	LACP is enabled or disabled on this port.

The following command shows an example of the command output for all ports.

```
(CN1610) #show port all

               Admin     Physical   Physical   Link   Link    LACP
Actor
Intf     Type   Mode      Mode       Status     Status Trap    Mode
Timeout
--------- ------ --------- ---------- ---------- ------ ------- ---
--- --------
0/1            Enable    Auto       100 Full   Up     Enable  Enable
long
0/2            Enable    Auto       100 Full   Up     Enable  Enable
long
0/3            Enable    Auto                  Down   Enable  Enable
long
0/4            Enable    Auto       100 Full   Up     Enable  Enable
long
0/5            Enable    Auto       100 Full   Up     Enable  Enable
long
0/6            Enable    Auto       100 Full   Up     Enable  Enable
long
0/7            Enable    Auto       100 Full   Up     Enable  Enable
long
0/8            Enable    Auto       100 Full   Up     Enable  Enable
long
1/1            Enable                          Down   Disable N/A
N/A
1/2            Enable                          Down   Disable N/A
N/A
1/3            Enable                          Down   Disable N/A
N/A
1/4            Enable                          Down   Disable N/A
N/A
1/5            Enable                          Down   Disable N/A
N/A
1/6            Enable                          Down   Disable N/A
N/A
```

The following command shows an example of the command output for a range of ports.

```
(CN1610) #show port 0/1-1/6

               Admin     Physical   Physical   Link   Link    LACP
Actor
Intf     Type   Mode      Mode       Status     Status Trap    Mode
Timeout
```

```
--------- ------ --------- ---------- ---------- ------ ------- ---
--- --------
0/1             Enable    Auto       100 Full   Up     Enable  Enable
long
0/2             Enable    Auto       100 Full   Up     Enable  Enable
long
0/3             Enable    Auto                  Down   Enable  Enable
long
0/4             Enable    Auto       100 Full   Up     Enable  Enable
long
0/5             Enable    Auto       100 Full   Up     Enable  Enable
long
0/6             Enable    Auto       100 Full   Up     Enable  Enable
long
0/7             Enable    Auto       100 Full   Up     Enable  Enable
long
0/8             Enable    Auto       100 Full   Up     Enable  Enable
long
1/1             Enable                          Down   Disable N/A
N/A
1/2             Enable                          Down   Disable N/A
N/A
1/3             Enable                          Down   Disable N/A
N/A
1/4             Enable                          Down   Disable N/A
N/A
1/5             Enable                          Down   Disable N/A
N/A
1/6             Enable                          Down   Disable N/A
N/A
```

show port advertise

Use this command to display the local administrative link advertisement configuration, local operational link advertisement, and the link partner advertisement for an interface. It also displays priority Resolution for speed and duplex as per 802.3 Annex 28B.3. It displays the Auto negotiation state, Phy Master/Slave Clock configuration, and Link state of the port.

If the link is down, the Clock is displayed as *No Link*, and a dash is displayed against the Oper Peer advertisement, and Priority Resolution. If Auto negotiation is disabled, then the admin Local Link advertisement, operational local link advertisement, operational peer advertisement, and Priority resolution fields are not displayed.

If this command is executed without the optional slot/port parameter, then it displays the Auto-negotiation state and operational Local link advertisement for all the ports. Operational link advertisement will display speed only if it is supported by both local as well as link partner. If auto-negotiation is disabled, then operational local link advertisement is not displayed.

Format	`show port advertise [slot/port]`
Mode	Privileged EXEC

The following commands show the command output with and without the optional parameter:

```
(Broadcom FASTPATH Switching)#show port advertise 0/1

Port: 0/1
Type: Gigabit - Level
Link State: Down
Auto Negotiation: Enabled
Clock: Auto
                              1000f 1000h 100f 100h 10f 10h
                              ----- ----- ---- ---- --- ---
Admin Local Link Advertisement no    no    yes  no   yes no
Oper Local Link Advertisement  no    no    yes  no   yes no
Oper Peer Advertisement        no    no    yes  yes  yes yes
Priority Resolution            -     -     yes  -    -   -

(Broadcom FASTPATH Switching)#show port advertise

Port      Type                                Neg      Operational
Link Advertisement
--------- ------------------------------ ----------- --------------
----------------
0/1   Gigabit - Level                   Enabled  1000f, 100f, 100h,
10f, 10h
0/2   Gigabit - Level                   Enabled  1000f, 100f, 100h,
10f, 10h
0/3   Gigabit - Level                   Enabled  1000f, 100f, 100h,
10f, 10h
```

show port description

This command displays the interface description. Instead of slot/port, `lag` *`lag-intf-num`* can be used as an alternate way to specify the LAG interface. `lag` *`lag-intf-num`* can also be used to specify the LAG interface where *`lag-intf-num`* is the LAG port number.

Format	`show port description slot/port`
Mode	Privileged EXEC

Term	Definition
Interface	slot/port
ifIndex	The interface index number associated with the port.
Description	The alpha-numeric description of the interface created by the command “description” on page 310.
MAC address	The MAC address of the port. The format is 6 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB.
Bit Offset Val	The bit offset value.

The following shows example CLI display output for the command.

```
(Broadcom FASTPATH Switching) #show port description 0/1

Interface...........0/1
ifIndex.............1
Description.........
MAC address.........00:10:18:82:0C:10
Bit Offset Val......1
```

Spanning Tree Protocol Commands

This section describes the commands you use to configure Spanning Tree Protocol (STP). STP helps prevent network loops, duplicate messages, and network instability.

Note
STP is enabled on the switch and on all ports and LAGs by default.

Note
If STP is disabled, the system does not forward BPDU messages.

spanning-tree

This command sets the spanning-tree operational mode to enabled.

Default	enabled
Format	`spanning-tree`
Mode	Global Config

no spanning-tree

This command sets the spanning-tree operational mode to disabled. While disabled, the spanning-tree configuration is retained and can be changed, but is not activated.

Format	`no spanning-tree`
Mode	Global Config

spanning-tree auto-edge

Use this command to allow the interface to become an edge port if it does not receive any BPDUs within a given amount of time.

Default	Enabled
Format	`spanning-tree auto-edge`
Mode	Interface Config

no spanning-tree auto-edge

This command resets the auto-edge status of the port to the default value.

Format	`no spanning-tree auto-edge`
Mode	Interface Config

spanning-tree backbonefast

Use this command to enable the detection of indirect link failures and accelerate spanning tree convergence on PVSTP configured switches.

Backbonefast accelerates finding an alternate path when an indirect link to the root port goes down.

Backbonefast can be configured even if the switch is configured for MST(RSTP) or PVST mode. It only has an effect when the switch is configured for the PVST mode.

If a backbonefast-enabled switch receives an inferior BPDU from its designated switch on a root or blocked port, it sets the maximum aging time on the interfaces on which it received the inferior BPDU if there are alternate paths to the designated switch. This allows a blocked port to immediately move to the listening state where the port can be transitioned to the forwarding state in the normal manner.

On receipt of an inferior BPDU from a designated bridge, backbonefast enabled switches send a Root Link Query (RLQ) request to all non-designated ports except the port from which it received the inferior BPDU. This check validates that the switch can receive packets from the root on ports where it expects to receive BPDUs. The port from which the original inferior BPDU was received is excluded because it has already encountered a failure. Designated ports are excluded as they do not lead to the root.

On receipt of an RLQ response, if the answer is negative, the receiving port has lost connection to the root and its BPDU is immediately aged out. If all nondesignated ports have already received a negative answer, the whole bridge has lost the root and can start the STP calculation from scratch.

If the answer confirms the switch can access the root bridge on a port, it can immediately age out the port on which it initially received the inferior BPDU.

A bridge that sends an RLQ puts its bridge ID in the PDU. This ensures that it does not flood the response on designated ports.

A bridge that receives an RLQ and has connectivity to the root forwards the query toward the root through its root port.

A bridge that receives a RLQ request and does not have connectivity to the root (switch bridge ID is different from the root bridge ID in the query) or is the root bridge immediately answers the query with its root bridge ID.

RLQ responses are flooded on designated ports.

Default	NA
Format	`spanning-tree backbonefast`
Mode	Global Config

no spanning-tree backbonefast

This command disables backbonefast.

Note
PVRSTP embeds support for FastBackbone and FastUplink. Even if FastUplink and FastBackbone are configured, they are effective only in PVSTP mode.

Format	`no spanning-tree backbonefast`
Mode	Global Config

spanning-tree bpdufilter

Use this command to enable BPDU Filter on an interface or range of interfaces.

Default	disabled
Format	`spanning-tree bpdufilter`
Mode	Interface Config

no spanning-tree bpdufilter

Use this command to disable BPDU Filter on the interface or range of interfaces.

Default	disabled
Format	`no spanning-tree bpdufilter`
Mode	Interface Config

spanning-tree bpdufilter default

Use this command to enable BPDU Filter on all the edge port interfaces.

Default	disabled
Format	`spanning-tree bpdufilter default`
Mode	Global Config

no spanning-tree bpdufilter default

Use this command to disable BPDU Filter on all the edge port interfaces.

Default	disabled
Format	`no spanning-tree bpdufilter default`
Mode	Global Config

spanning-tree bpduflood

Use this command to enable BPDU Flood on an interface or range of interfaces.

Default	disabled
Format	`spanning-tree bpduflood`
Mode	Interface Config

no spanning-tree bpduflood

Use this command to disable BPDU Flood on the interface or range of interfaces.

Default	disabled
Format	`no spanning-tree bpduflood`
Mode	Interface Config

spanning-tree bpduguard

Use this command to enable BPDU Guard on the switch.

Default	disabled
Format	`spanning-tree bpduguard`

Mode	Global Config

no spanning-tree bpduguard

Use this command to disable BPDU Guard on the switch.

Default	disabled
Format	`no spanning-tree bpduguard`
Mode	Global Config

spanning-tree bpdumigrationcheck

Use this command to force a transmission of rapid spanning tree (RSTP) and multiple spanning tree (MSTP) BPDUs. Use the slot/port parameter to transmit a BPDU from a specified interface, or use the *all* keyword to transmit RST or MST BPDUs from all interfaces. This command forces the BPDU transmission when you execute it, so the command does not change the system configuration or have a **no** version.

Format	`spanning-tree bpdumigrationcheck {slot/port | all}`
Mode	Global Config

spanning-tree configuration name

This command sets the Configuration Identifier Name for use in identifying the configuration that this switch is currently using. The *name* is a string of up to 32 characters.

Default	base MAC address in hexadecimal notation
Format	`spanning-tree configuration name` *name*
Mode	Global Config

no spanning-tree configuration name

This command resets the Configuration Identifier Name to its default.

Format	`no spanning-tree configuration name`
Mode	Global Config

spanning-tree configuration revision

This command sets the Configuration Identifier Revision Level for use in identifying the configuration that this switch is currently using. The Configuration Identifier Revision Level is a number in the range of 0 to 65535.

Default	0
Format	`spanning-tree configuration revision` *`0-65535`*
Mode	Global Config

no spanning-tree configuration revision

This command sets the Configuration Identifier Revision Level for use in identifying the configuration that this switch is currently using to the default value.

Format	`no spanning-tree configuration revision`
Mode	Global Config

spanning-tree cost

Use this command to configure the external path cost for port used by a MST instance. When the `auto` keyword is used, the path cost from the port to the root bridge is automatically determined by the speed of the interface. To configure the cost manually, specify a *`cost`* value from 1–200000000.

Default	auto
Format	`spanning-tree cost {`*`cost`* `| auto}`
Mode	Interface Config

no spanning-tree cost

This command resets the auto-edge status of the port to the default value.

Format	`no spanning-tree cost`
Mode	Interface Config

spanning-tree edgeport

This command specifies that an interface (or range of interfaces) is an Edge Port within the common and internal spanning tree. This allows this port to transition to Forwarding State without delay.

Format	`spanning-tree edgeport`
Mode	Interface Config

no spanning-tree edgeport

This command specifies that this port is not an Edge Port within the common and internal spanning tree.

Format	`no spanning-tree edgeport`
Mode	Interface Config

spanning-tree forceversion

This command sets the Force Protocol Version parameter to a new value.

Default	802.1s
Format	`spanning-tree forceversion {802.1d | 802.1s | 802.1w}`
Mode	Global Config

- Use 802.1d to specify that the switch transmits ST BPDUs rather than MST BPDUs (IEEE 802.1d functionality supported).
- Use 802.1s to specify that the switch transmits MST BPDUs (IEEE 802.1s functionality supported).
- Use 802.1w to specify that the switch transmits RST BPDUs rather than MST BPDUs (IEEE 802.1w functionality supported).

no spanning-tree forceversion

This command sets the Force Protocol Version parameter to the default value.

Format	`no spanning-tree forceversion`
Mode	Global Config

spanning-tree forward-time

This command sets the Bridge Forward Delay parameter to a new value for the common and internal spanning tree. The forward-time value is in seconds within a range of 4 to 30, with the value being greater than or equal to "(Bridge Max Age / 2) + 1".

Default	15
Format	`spanning-tree forward-time` *`4-30`*
Mode	Global Config

no spanning-tree forward-time

This command sets the Bridge Forward Delay parameter for the common and internal spanning tree to the default value.

Format	`no spanning-tree forward-time`
Mode	Global Config

spanning-tree guard

This command selects whether loop guard or root guard is enabled on an interface or range of interfaces. If neither is enabled, then the port operates in accordance with the multiple spanning tree protocol.

Default	none
Format	`spanning-tree guard {none | root | loop}`
Mode	Interface Config

no spanning-tree guard

This command disables loop guard or root guard on the interface.

Format	`no spanning-tree guard`
Mode	Interface Config

spanning-tree max-age

This command sets the Bridge Max Age parameter to a new value for the common and internal spanning tree. The max-age value is in seconds within a range of 6 to 40, with the value being less than or equal to *2 x (Bridge Forward Delay - 1)*.

Default	20
Format	`spanning-tree max-age` *`6-40`*
Mode	Global Config

no spanning-tree max-age

This command sets the Bridge Max Age parameter for the common and internal spanning tree to the default value.

Format	`no spanning-tree max-age`
Mode	Global Config

spanning-tree max-hops

This command sets the Bridge Max Hops parameter to a new value for the common and internal spanning tree. The max-hops value is a range from 6 to 40.

Default	20
Format	`spanning-tree max-hops` *`6-40`*
Mode	Global Config

no spanning-tree max-hops

This command sets the Bridge Max Hops parameter for the common and internal spanning tree to the default value.

Format	`no spanning-tree max-hops`
Mode	Global Config

spanning-tree mode

This command configures global spanning tree mode per VLAN spanning tree. On a switch, only one mode can be enabled at a time.

When PVSTP or rapid PVSTP (PVRSTP) is enabled, MSTP/RSTP/STP is operationally disabled. To reenable MSTP/RSTP/STP, disable PVSTP/PVRSTP. By default, FASTPATH has MSTP enabled. In PVSTP or PVRSTP mode, BPDUs contain per-VLAN information instead of the common spanning-tree information (MST/RSTP).

PVSTP maintains independent spanning tree information about each configured VLAN. PVSTP uses IEEE 802.1Q trunking and allows a trunked VLAN to maintain blocked or forwarding state per port on a per-VLAN basis. This allows a trunk port to be forwarded on some VLANs and blocked on other VLANs.

PVRSTP is based on the IEEE 8012.1w standard. It supports fast convergence IEEE 802.1D. PVRSTP is compatible with IEEE 802.1D spanning tree. PVRSTP sends BPDUs on all ports, instead of only the root bridge sending BPDUs, and supports the discarding, learning, and forwarding states.

When the mode is changed to PVRSTP, version 0 STP BPDUs are no longer transmitted and version 2 PVRSTP BPDUs that carry per-VLAN information are transmitted on the VLANs enabled for spanning-tree. If a version 0 BPDU is seen, PVRSTP reverts to sending version 0 BPDUs.

Per VLAN Rapid Spanning Tree Protocol (PVRSTP) embeds support for PVSTP FastBackbone and FastUplink. There is no provision to enable or disable these features in PVRSTP.

Default	Disabled
Format	`spanning-tree mode {pvst|rapid-pvst}`
Mode	Global Config

no spanning-tree mode

This command globally configures the switch to the default FASTPATH spanning-tree mode, MSTP.

Format	`no spanning-tree mode { pvst | rapid-pvst }`
Mode	Global Configuration

spanning-tree mst

This command sets the Path Cost or Port Priority for this port within the multiple spanning tree instance or in the common and internal spanning tree. If you specify an *mstid* parameter that corresponds to an existing multiple spanning

tree instance, the configurations are done for that multiple spanning tree instance. If you specify 0 (defined as the default CIST ID) as the *mstid*, the configurations are done for the common and internal spanning tree instance.

If you specify the **cost** option, the command sets the path cost for this port within a multiple spanning tree instance or the common and internal spanning tree instance, depending on the *mstid* parameter. You can set the path cost as a number in the range of 1 to 200000000 or **auto**. If you select **auto** the path cost value is set based on Link Speed.

If you specify the **port-priority** option, this command sets the priority for this port within a specific multiple spanning tree instance or the common and internal spanning tree instance, depending on the *mstid* parameter. The port-priority value is a number in the range of 0 to 240 in increments of 16.

Default	◆ cost—auto ◆ port-priority—128
Format	`spanning-tree mst` *`mstid`* {{`cost` *`1-200000000`* | `auto`} | `port-priority` *`0-240`*}
Mode	Interface Config

no spanning-tree mst

This command sets the Path Cost or Port Priority for this port within the multiple spanning tree instance, or in the common and internal spanning tree to the respective default values. If you specify an *mstid* parameter that corresponds to an existing multiple spanning tree instance, you are configuring that multiple spanning tree instance. If you specify 0 (defined as the default CIST ID) as the *mstid*, you are configuring the common and internal spanning tree instance.

If the you specify **cost**, this command sets the path cost for this port within a multiple spanning tree instance or the common and internal spanning tree instance, depending on the *mstid* parameter, to the default value, i.e., a path cost value based on the Link Speed.

If you specify **port-priority**, this command sets the priority for this port within a specific multiple spanning tree instance or the common and internal spanning tree instance, depending on the *mstid* parameter, to the default value.

Format	`no spanning-tree mst` *`mstid`* {`cost` | `port-priority`}
Mode	Interface Config

spanning-tree mst instance

This command adds a multiple spanning tree instance to the switch. The parameter *mstid* is a number within a range of 1 to 4094, that corresponds to the new instance ID to be added. The maximum number of multiple instances supported by the switch is 4.

Default	none
Format	`spanning-tree mst instance` *mstid*
Mode	Global Config

no spanning-tree mst instance

This command removes a multiple spanning tree instance from the switch and reallocates all VLANs allocated to the deleted instance to the common and internal spanning tree. The parameter *mstid* is a number that corresponds to the desired existing multiple spanning tree instance to be removed.

Format	`no spanning-tree mst instance` *mstid*
Mode	Global Config

spanning-tree mst priority

This command sets the bridge priority for a specific multiple spanning tree instance. The parameter *mstid* is a number that corresponds to the desired existing multiple spanning tree instance. The priority value is a number within a range of 0 to 4094.

If you specify 0 (defined as the default CIST ID) as the *mstid*, this command sets the Bridge Priority parameter to a new value for the common and internal spanning tree. The bridge priority value is a number within a range of 0 to 4094. The twelve least significant bits are masked according to the 802.1s specification. This causes the priority to be rounded down to the next lower valid priority.

Default	32768
Format	`spanning-tree mst priority` *mstid 0-4094*
Mode	Global Config

no spanning-tree mst priority

This command sets the bridge priority for a specific multiple spanning tree instance to the default value. The parameter *mstid* is a number that corresponds to the desired existing multiple spanning tree instance.

If 0 (defined as the default CIST ID) is passed as the *mstid*, this command sets the Bridge Priority parameter for the common and internal spanning tree to the default value.

Format	`no spanning-tree mst priority` *mstid*
Mode	Global Config

spanning-tree mst vlan

This command adds an association between a multiple spanning tree instance and one or more VLANs so that the VLAN(s) are no longer associated with the common and internal spanning tree. The parameter *mstid* is a multiple spanning tree instance identifier, in the range of 0 to 4094, that corresponds to the desired existing multiple spanning tree instance. The *vlanid* can be specified as a single VLAN, a list, or a range of values. To specify a list of VLANs, enter a list of VLAN IDs in the range 1 to 4093, each separated by a comma with no spaces in between. To specify a range of VLANs, separate the beginning and ending VLAN ID with a dash (-). Spaces and zeros are not permitted. The VLAN IDs may or may not exist in the system.

Format	`spanning-tree mst vlan` *mstid vlanid*
Mode	Global Config

no spanning-tree mst vlan

This command removes an association between a multiple spanning tree instance and one or more VLANs so that the VLAN(s) are again associated with the common and internal spanning tree.

Format	`no spanning-tree mst vlan` *mstid vlanid*
Mode	Global Config

spanning-tree port mode

This command sets the Administrative Switch Port State for this port to enabled for use by spanning tree.

Default	enabled
Format	`spanning-tree port mode`
Mode	Interface Config

no spanning-tree port mode

This command sets the Administrative Switch Port State for this port to disabled, disabling the port for use by spanning tree.

Format	`no spanning-tree port mode`
Mode	Interface Config

spanning-tree port mode all

This command sets the Administrative Switch Port State for all ports to enabled.

Default	enabled
Format	`spanning-tree port mode all`
Mode	Global Config

no spanning-tree port mode all

This command sets the Administrative Switch Port State for all ports to disabled.

Format	`no spanning-tree port mode all`
Mode	Global Config

spanning-tree port-priority

Use this command to change the priority value of the port to allow the operator to select the relative importance of the port in the forwarding process. Set this value to a lower number to prefer a port for forwarding of frames.

All LAN ports have 128 as priority value by default. PVSTP/PVRSTP puts the LAN port with the lowest LAN port number in the forwarding state and blocks other LAN ports.

The application uses the port priority value when the LAN port is configured as an edge port.

Default	enabled
Format	`spanning-tree port-priority` *`0-240`*
Mode	Interface Config

spanning-tree tcnguard

Use this command to enable TCN guard on the interface. When enabled, TCN Guard restricts the interface from propagating any topology change information received through that interface.

Default	Enabled
Format	`spanning-tree tcnguard`
Mode	Interface Config

no spanning-tree tcnguard

This command resets the TCN guard status of the port to the default value.

Format	`no spanning-tree tcnguard`
Mode	Interface Config

spanning-tree transmit

This command sets the Bridge Transmit Hold Count parameter.

Default	`6`
Format	`spanning-tree transmit` *`hold-count`*
Mode	Global Config

Parameter	Description
hold-count	The Bridge Tx hold-count parameter. The value in an integer between 1 and 10.

spanning-tree uplinkfast

Use this command to configure the rate at which gratuitous frames are sent (in packets per second) after switchover to an alternate port on PVSTP configured switches and enables uplinkfast on PVSTP switches. The range is 0-32000; the default is 150. This command has the effect of accelerating spanning-tree convergence after switchover to an alternate port.

Uplinkfast can be configured even if the switch is configured for MST(RSTP) mode, but it only has an effect when the switch is configured for PVST mode. Enabling FastUplink increases the priority by 3000. Path costs less than 3000 have an additional 3000 added when uplinkfast is enabled. This reduces the probability that the switch will become the root switch.

Uplinkfast immediately changes to an alternate root port on detecting a root port failure and changes the new root port directly to the fowarding state. A TCN is sent for this event.

After a switchover to an alternate port (new root port), uplinkfast multicasts a gratuitous frame on the new root port on behalf of each attached machine so that the rest of the network knows to use the secondary link to reach that machine.

PVRSTP embeds support for backbonefast and uplinkfast. There is no provision to enable or disable these features in PVRSTP configured switches.

Default	`150`
Format	`spanning-tree uplinkfast [max-update-rate` *`packets`*`]`
Mode	Global Config

no spanning-tree uplinkfast

This command disables uplinkfast on PVSTP configured switches. All switch priorities and path costs that have not been modified from their default values are set to their default values.

Format	`no spanning-tree uplinkfast [max-update-rate]`
Mode	Global Config

show spanning-tree

This command displays spanning tree settings for the common and internal spanning tree. The following details are displayed.

Format	`show spanning-tree`

Mode	◆ Privileged EXEC ◆ User EXEC

Term	Definition
Bridge Priority	Specifies the bridge priority for the Common and Internal Spanning tree (CST). The value lies between 0 and 61440. It is displayed in multiples of 4096.
Bridge Identifier	The bridge identifier for the CST. It is made up using the bridge priority and the base MAC address of the bridge.
Time Since Topology Change	Time in seconds.
Topology Change Count	Number of times changed.
Topology Change in Progress	Boolean value of the Topology Change parameter for the switch indicating if a topology change is in progress on any port assigned to the common and internal spanning tree.
Designated Root	The bridge identifier of the root bridge. It is made up from the bridge priority and the base MAC address of the bridge.
Root Path Cost	Value of the Root Path Cost parameter for the common and internal spanning tree.
Root Port Identifier	Identifier of the port to access the Designated Root for the CST
Bridge Max Age	Derived value.
Bridge Max Hops	Bridge max-hops count for the device.
Root Port Bridge Forward Delay	Derived value.
Hello Time	Configured value of the parameter for the CST.

Term	Definition
Bridge Hold Time	Minimum time between transmission of Configuration Bridge Protocol Data Units (BPDUs).
CST Regional Root	Bridge Identifier of the CST Regional Root. It is made up using the bridge priority and the base MAC address of the bridge.
Regional Root Path Cost	Path Cost to the CST Regional Root.
Associated FIDs	List of forwarding database identifiers currently associated with this instance.
Associated VLANs	List of VLAN IDs currently associated with this instance.

The following shows example CLI display output for the command.

```
(CN1610) #show spanning-tree

Bridge Priority.............................. 32768
Bridge Identifier.............................
80:00:00:10:18:48:FC:07
Time Since Topology Change..................... 8 day 3 hr 22 min
37 sec
Topology Change Count.......................... 0
Topology Change in progress.................... FALSE
Designated Root...............................
80:00:00:10:18:48:FC:07
Root Path Cost................................. 0
Root Port Identifier........................... 00:00
Bridge Max Age................................. 20
Bridge Max Hops................................ 20
Bridge Tx Hold Count........................... 6
Bridge Forwarding Delay........................ 15
Hello Time..................................... 2
Bridge Hold Time............................... 6
CST Regional Root.............................
80:00:00:10:18:48:FC:07
Regional Root Path Cost........................ 0

     Associated FIDs           Associated VLANs
     ---------------           ----------------
```

```
(CN1610) #
```

show spanning-tree backbonefast

This command displays spanning tree information for backbonefast.

Format	`show spanning-tree backbonefast`
Mode	◆ Privileged EXEC ◆ User EXEC

Term	Definition
Transitions via Backbonefast	The number of backbonefast transitions.
Inferior BPDUs received (all VLANs)	The number of inferior BPDUs received on all VLANs.
RLQ request PDUs received (all VLANs)	The number of root link query (RLQ) requests PDUs received on all VLANs.
RLQ response PDUs received (all VLANs)	The number of RLQ response PDUs received on all VLANs.
RLQ request PDUs sent (all VLANs)	The number of RLQ request PDUs sent on all VLANs.
RLQ response PDUs sent (all VLANs)	The number of RLQ response PDUs sent on all VLANs.

The following shows example output from the command.

```
(CN1610)#show spanning-tree backbonefast

Backbonefast Statistics
-----------------------
Transitions via Backbonefast (all VLANs)          : 0
Inferior BPDUs received (all VLANs)               : 0
RLQ request PDUs received (all VLANs)             : 0
RLQ response PDUs received (all VLANs)            : 0
RLQ request PDUs sent (all VLANs)                 : 0
RLQ response PDUs sent (all VLANs)                : 0
```

show spanning-tree brief

This command displays spanning tree settings for the bridge. The following information appears.

Format	`show spanning-tree brief`
Mode	◆ Privileged EXEC ◆ User EXEC

Term	Definition
Bridge Priority	Configured value.
Bridge Identifier	The bridge identifier for the selected MST instance. It is made up using the bridge priority and the base MAC address of the bridge.
Bridge Max Age	Configured value.
Bridge Max Hops	Bridge max-hops count for the device.
Bridge Hello Time	Configured value.
Bridge Forward Delay	Configured value.
Bridge Hold Time	Minimum time between transmission of Configuration Bridge Protocol Data Units (BPDUs).

The following shows example CLI display output for the command.

```
(CN1610) #show spanning-tree brief

Bridge Priority.............................. 32768
Bridge Identifier.............................
80:00:00:10:18:48:FC:07
Bridge Max Age............................... 20
Bridge Max Hops.............................. 20
Bridge Hello Time............................ 2
Bridge Forward Delay......................... 15
Bridge Hold Time............................. 6

(CN1610) #
```

show spanning-tree interface

This command displays the settings and parameters for a specific switch port within the common and internal spanning tree. The slot/port is the desired switch port. Instead of slot/port, `lag` *`lag-intf-num`* can be used as an alternate way to specify the LAG interface. `lag` *`lag-intf-num`* can also be used to specify the LAG interface where *`lag-intf-num`* is the LAG port number. The following details are displayed on execution of the command.

Format	`show spanning-tree interface {slot/port|lag lag-intf-num}`
Mode	◆ Privileged EXEC ◆ User EXEC

Term	Definition
Hello Time	Admin hello time for this port.
Port Mode	Enabled or disabled.
BPDU Guard Effect	Enabled or disabled.
Root Guard	Enabled or disabled.
Loop Guard	Enabled or disabled.
TCN Guard	Enable or disable the propagation of received topology change notifications and topology changes to other ports.
BPDU Filter Mode	Enabled or disabled.
BPDU Flood Mode	Enabled or disabled.
Auto Edge	To enable or disable the feature that causes a port that has not seen a BPDU for **edge delay** time, to become an edge port and transition to forwarding faster.
Port Up Time Since Counters Last Cleared	Time since port was reset, displayed in days, hours, minutes, and seconds.
STP BPDUs Transmitted	Spanning Tree Protocol Bridge Protocol Data Units sent.

Term	Definition
STP BPDUs Received	Spanning Tree Protocol Bridge Protocol Data Units received.
RSTP BPDUs Transmitted	Rapid Spanning Tree Protocol Bridge Protocol Data Units sent.
RSTP BPDUs Received	Rapid Spanning Tree Protocol Bridge Protocol Data Units received.
MSTP BPDUs Transmitted	Multiple Spanning Tree Protocol Bridge Protocol Data Units sent.
MSTP BPDUs Received	Multiple Spanning Tree Protocol Bridge Protocol Data Units received.

The following shows example CLI display output for the command.

```
(CN1610) >show spanning-tree interface 0/1

Hello Time..................................... Not Configured
Port Mode...................................... Enabled
BPDU Guard Effect.............................. Disabled
Root Guard..................................... FALSE
Loop Guard..................................... FALSE
TCN Guard...................................... FALSE
BPDU Filter Mode............................... Disabled
BPDU Flood Mode................................ Disabled
Auto Edge...................................... TRUE
Port Up Time Since Counters Last Cleared....... 8 day 3 hr 39 min 58
sec
STP BPDUs Transmitted.......................... 0
STP BPDUs Received............................. 0
RSTP BPDUs Transmitted......................... 0
RSTP BPDUs Received............................ 0
MSTP BPDUs Transmitted......................... 0
MSTP BPDUs Received............................ 0

(CN1610) >
```

The following shows example CLI display output for the command.

```
(CN1610) >show spanning-tree interface lag 1

Hello Time..................................... Not Configured
```

```
Port Mode..................................... Enabled
BPDU Guard Effect............................. Disabled
Root Guard.................................... FALSE
Loop Guard.................................... FALSE
TCN Guard..................................... FALSE
BPDU Filter Mode.............................. Disabled
BPDU Flood Mode............................... Disabled
Auto Edge..................................... TRUE
Port Up Time Since Counters Last Cleared....... 8 day 3 hr 42 min 5
sec
STP BPDUs Transmitted......................... 0
STP BPDUs Received............................ 0
RSTP BPDUs Transmitted........................ 0
RSTP BPDUs Received........................... 0
MSTP BPDUs Transmitted........................ 0
MSTP BPDUs Received........................... 0

(CN1610) >
```

show spanning-tree mst detailed

This command displays the detailed settings for an MST instance.

Format	`show spanning-tree mst detailed` *mstid*
Mode	◆ Privileged EXEC ◆ User EXEC

Parameter	Description
mstid	A multiple spanning tree instance identifier. The value is 0–4094.

The following shows example CLI display output for the command.

```
(CN1610) >show spanning-tree mst detailed 0

MST Instance ID............................... 0
MST Bridge Priority........................... 32768
MST Bridge Identifier.........................
80:00:00:10:18:48:FC:07
Time Since Topology Change..................... 8 day 3 hr 47 min 7
sec
Topology Change Count......................... 0
Topology Change in progress................... FALSE
```

```
Designated Root.............................
80:00:00:10:18:48:FC:07
Root Path Cost.............................. 0
Root Port Identifier.......................... 00:00

     Associated FIDs           Associated VLANs
     ---------------           ----------------

(CN1610) >
```

show spanning-tree mst port detailed

This command displays the detailed settings and parameters for a specific switch port within a particular multiple spanning tree instance. The parameter *mstid* is a number that corresponds to the desired existing multiple spanning tree instance. The slot/port is the desired switch port. Instead of slot/port, *lag lag-intf-num* can be used as an alternate way to specify the LAG interface. *lag lag-intf-num* can also be used to specify the LAG interface where *lag-intf-num* is the LAG port number.

Format	show spanning-tree mst port detailed *mstid* {slot/port|*lag lag-intf-num*}
Mode	◆ Privileged EXEC ◆ User EXEC

Term	Definition
MST Instance ID	The ID of the existing multiple spanning tree (MST) instance identifier. The value is 0–4094.
Port Identifier	The port identifier for the specified port within the selected MST instance. It is made up from the port priority and the interface number of the port.
Port Priority	The priority for a particular port within the selected MST instance. The port priority is displayed in multiples of 16.
Port Forwarding State	Current spanning tree state of this port.

Term	Definition
Port Role	Each enabled MST Bridge Port receives a Port Role for each spanning tree. The port role is one of the following values: Root Port, Designated Port, Alternate Port, Backup Port, Master Port or Disabled Port
Auto-Calculate Port Path Cost	Indicates whether auto calculation for port path cost is enabled.
Port Path Cost	Configured value of the Internal Port Path Cost parameter.
Designated Root	The Identifier of the designated root for this port.
Root Path Cost	The path cost to get to the root bridge for this instance. The root path cost is zero if the bridge is the root bridge for that instance.
Designated Bridge	Bridge Identifier of the bridge with the Designated Port.
Designated Port Identifier	Port on the Designated Bridge that offers the lowest cost to the LAN.
Loop Inconsistent State	The current loop inconsistent state of this port in this MST instance. When in loop inconsistent state, the port has failed to receive BPDUs while configured with loop guard enabled. Loop inconsistent state maintains the port in a blocking state until a subsequent BPDU is received.
Transitions Into Loop Inconsistent State	The number of times this interface has transitioned into loop inconsistent state.
Transitions Out of Loop Inconsistent State	The number of times this interface has transitioned out of loop inconsistent state.

If you specify 0 (defined as the default CIST ID) as the *mstid*, this command displays the settings and parameters for a specific switch port within the common and internal spanning tree. The slot/port is the desired switch port. In this case, the following are displayed.

Term	Definition
Port Identifier	The port identifier for this port within the CST.
Port Priority	The priority of the port within the CST.
Port Forwarding State	The forwarding state of the port within the CST.
Port Role	The role of the specified interface within the CST.
Auto-Calculate Port Path Cost	Indicates whether auto calculation for port path cost is enabled or not (disabled).
Port Path Cost	The configured path cost for the specified interface.
Auto-Calculate External Port Path Cost	Indicates whether auto calculation for external port path cost is enabled.
External Port Path Cost	The cost to get to the root bridge of the CIST across the boundary of the region. This means that if the port is a boundary port for an MSTP region, then the external path cost is used.
Designated Root	Identifier of the designated root for this port within the CST.
Root Path Cost	The root path cost to the LAN by the port.
Designated Bridge	The bridge containing the designated port.
Designated Port Identifier	Port on the Designated Bridge that offers the lowest cost to the LAN.
Topology Change Acknowledgement	Value of flag in next Configuration Bridge Protocol Data Unit (BPDU) transmission indicating if a topology change is in progress for this port.
Hello Time	The hello time in use for this port.
Edge Port	The configured value indicating if this port is an edge port.
Edge Port Status	The derived value of the edge port status. True if operating as an edge port; false otherwise.

Term	Definition
Point To Point MAC Status	Derived value indicating if this port is part of a point to point link.
CST Regional Root	The regional root identifier in use for this port.
CST Internal Root Path Cost	The internal root path cost to the LAN by the designated external port.
Loop Inconsistent State	The current loop inconsistent state of this port in this MST instance. When in loop inconsistent state, the port has failed to receive BPDUs while configured with loop guard enabled. Loop inconsistent state maintains the port in a blocking state until a subsequent BPDU is received.
Transitions Into Loop Inconsistent State	The number of times this interface has transitioned into loop inconsistent state.
Transitions Out of Loop Inconsistent State	The number of times this interface has transitioned out of loop inconsistent state.

The following shows example CLI display output for the command in *slot/port* format.

```
(CN1610) >show spanning-tree mst port detailed 0 0/1

Port Identifier.............................. 80:01
Port Priority................................ 128
Port Forwarding State........................ Disabled
Port Role.................................... Disabled
Auto-calculate Port Path Cost................ Enabled
Port Path Cost............................... 0
Auto-Calculate External Port Path Cost....... Enabled
External Port Path Cost...................... 0
Designated Root..............................
80:00:00:10:18:48:FC:07
Root Path Cost............................... 0
Designated Bridge............................
80:00:00:10:18:48:FC:07
Designated Port Identifier................... 00:00
Topology Change Acknowledge.................. FALSE
Hello Time................................... 2
```

```
Edge Port..................................... FALSE
Edge Port Status.............................. FALSE
Point to Point MAC Status..................... TRUE
CST Regional Root.............................
80:00:00:10:18:48:FC:07
CST Internal Root Path Cost................... 0
Loop Inconsistent State....................... FALSE
Transitions Into Loop Inconsistent State...... 0
Transitions Out Of Loop Inconsistent State..... 0
```

The following shows example CLI display output for the command using a LAG interface number.

```
(CN1610) >show spanning-tree mst port detailed 0 lag 1

Port Identifier.............................. 60:42
Port Priority................................ 96
Port Forwarding State........................ Disabled
Port Role.................................... Disabled
Auto-calculate Port Path Cost................ Enabled
Port Path Cost............................... 0
Auto-Calculate External Port Path Cost....... Enabled
External Port Path Cost...................... 0
Designated Root..............................
80:00:00:10:18:48:FC:07
Root Path Cost............................... 0
Designated Bridge............................
80:00:00:10:18:48:FC:07
Designated Port Identifier................... 00:00
Topology Change Acknowledge.................. FALSE
Hello Time................................... 2
Edge Port.................................... FALSE
Edge Port Status............................. FALSE
Point to Point MAC Status..................... TRUE
CST Regional Root.............................
80:00:00:10:18:48:FC:07
CST Internal Root Path Cost................... 0
Loop Inconsistent State....................... FALSE
Transitions Into Loop Inconsistent State...... 0
Transitions Out Of Loop Inconsistent State..... 0
--More-- or (q)uit

(CN1610) >
```

show spanning-tree mst port summary

This command displays the settings of one or all ports within the specified multiple spanning tree instance. The parameter *mstid* indicates a particular MST instance. The parameter {slot/port|all} indicates the desired switch port or all ports. Instead of slot/port, lag *lag-intf-num* can be used as an alternate way to specify the LAG interface. lag *lag-intf-num* can also be used to specify the LAG interface where *lag-intf-num* is the LAG port number.

If you specify 0 (defined as the default CIST ID) as the *mstid*, the status summary displays for one or all ports within the common and internal spanning tree.

Format	show spanning-tree mst port summary *mstid* {slot/port |lag *lag-intf-num*| all}
Mode	◆ Privileged EXEC ◆ User EXEC

Term	Definition
MST Instance ID	The MST instance associated with this port.
Interface	slot/port
STP Mode	Indicates whether spanning tree is enabled or disabled on the port.
Type	Currently not used.
STP State	The forwarding state of the port in the specified spanning tree instance.
Port Role	The role of the specified port within the spanning tree.
Desc	Indicates whether the port is in loop inconsistent state or not. This field is blank if the loop guard feature is not available.

The following shows example CLI display output for the command in *slot/port* format.

```
(CN1610) >show spanning-tree mst port summary 0 0/1

MST Instance ID.............................. CST
```

```
            STP                  STP            Port
Interface   Mode   Type          State          Role       Desc
--------- -------- ------- ----------------- ---------- ----------
0/1       Enabled          Disabled          Disabled
```

The following shows example CLI display output for the command using a LAG interface number.

```
(CN1610) >show spanning-tree mst port summary 0 lag 1

MST Instance ID.............................. CST

            STP                  STP            Port
Interface   Mode   Type          State          Role       Desc
--------- -------- ------- ----------------- ---------- ----------
3/1       Enabled          Disabled          Disabled
```

show spanning-tree mst port summary active

This command displays settings for the ports within the specified multiple spanning tree instance that are active links.

Format	`show spanning-tree mst port summary` *`mstid`* `active`
Mode	◆ Privileged EXEC ◆ User EXEC

Term	Definition
MST Instance ID	The ID of the existing MST instance.
Interface	slot/port
STP Mode	Indicates whether spanning tree is enabled or disabled on the port.
Type	Currently not used.
STP State	The forwarding state of the port in the specified spanning tree instance.

Term	Definition
Port Role	The role of the specified port within the spanning tree.
Desc	Indicates whether the port is in loop inconsistent state or not. This field is blank if the loop guard feature is not available.

The following shows example CLI display output for the command.

```
(CN1610) >show spanning-tree mst port summary 0 active

            STP                  STP            Port
Interface   Mode   Type          State          Role       Desc
--------- -------- ------- ---------------- ---------- ---------
```

show spanning-tree mst summary

This command displays summary information about all multiple spanning tree instances in the switch. On execution, the following details are displayed.

Format	`show spanning-tree mst summary`
Mode	◆ Privileged EXEC ◆ User EXEC

Term	Definition
MST Instance ID List	List of multiple spanning trees IDs currently configured.
For each MSTID: ◆ Associated FIDs ◆ Associated VLANs	◆ List of forwarding database identifiers associated with this instance. ◆ List of VLAN IDs associated with this instance.

show spanning-tree summary

This command displays spanning tree settings and parameters for the switch. The following details are displayed on execution of the command.

Format	`show spanning-tree summary`
Mode	◆ Privileged EXEC ◆ User EXEC

Term	**Definition**
Spanning Tree Adminmode	Enabled or disabled.
Spanning Tree Version	Version of 802.1 currently supported (IEEE 802.1s, IEEE 802.1w, or IEEE 802.1d) based upon the Force Protocol Version parameter.
BPDU Guard Mode	Enabled or disabled.
BPDU Filter Mode	Enabled or disabled.
Configuration Name	Identifier used to identify the configuration currently being used.
Configuration Revision Level	Identifier used to identify the configuration currently being used.
Configuration Digest Key	A generated Key used in the exchange of the BPDUs.
Configuration Format Selector	Specifies the version of the configuration format being used in the exchange of BPDUs. The default value is zero.
MST Instances	List of all multiple spanning tree instances configured on the switch.

The following shows example CLI display output for the command.

```
(CN1610) >show spanning-tree summary

Spanning Tree Adminmode.......... Enabled
Spanning Tree Version............. IEEE 802.1s
BPDU Guard Mode................... Disabled
BPDU Filter Mode.................. Disabled
Configuration Name................ ****
Configuration Revision Level...... ****
```

```
Configuration Digest Key.......... ****
Configuration Format Selector..... 0
No MST instances to display.
```

show spanning-tree uplinkfast

This command displays spanning tree information for uplinkfast.

Format	`show spanning-tree uplinkfast`
Mode	◆ Privileged EXEC ◆ User EXEC

Term	Definition
Uplinkfast transitions (all VLANs)	The number of uplinkfast transitions on all VLANs.
Proxy multicast addresses transmitted (all VLANs)	The number of proxy multicast addresses transmitted on all VLANs.

The following shows example output from the command.

```
(CN1610) #show spanning-tree uplinkfast

Uplinkfast is enabled.
BPDU update rate : 150 packets/sec

Uplinkfast Statistics
---------------------
Uplinkfast transitions (all VLANs)................. 0
Proxy multicast addresses transmitted (all VLANs).. 0
```

VLAN Commands

This section describes the commands you use to configure VLAN settings.

vlan database

This command gives you access to the VLAN Config mode, which allows you to configure VLAN characteristics

Format	`vlan database`
Mode	Privileged EXEC

network mgmt_vlan

This command configures the Management VLAN ID.

Default	1
Format	`network mgmt_vlan` *`1-4093`*
Mode	Privileged EXEC

no network mgmt_vlan

This command sets the Management VLAN ID to the default.

Format	`no network mgmt_vlan`
Mode	Privileged EXEC

vlan

This command creates a new VLAN and assigns it an ID. The ID is a valid VLAN identification number (ID 1 is reserved for the default VLAN). VLAN range is 2-4093.

Format	`vlan` *`2-4093`*
Mode	VLAN Config

no vlan

This command deletes an existing VLAN. The ID is a valid VLAN identification number (ID 1 is reserved for the default VLAN). The VLAN range is 2-4093.

Format	`no vlan 2-4093`
Mode	VLAN Config

vlan acceptframe

This command sets the frame acceptance mode on an interface or range of interfaces. For VLAN Only mode, untagged frames or priority frames received on this interface are discarded. For Admit All mode, untagged frames or priority frames received on this interface are accepted and assigned the value of the interface VLAN ID for this port. For admituntaggedonly mode, only untagged frames are accepted on this interface; tagged frames are discarded. With any option, VLAN tagged frames are forwarded in accordance with the IEEE 802.1Q VLAN Specification.

Default	all
Format	`vlan acceptframe {admituntaggedonly | vlanonly | all}`
Mode	Interface Config

no vlan acceptframe

This command resets the frame acceptance mode for the interface or range of interfaces to the default value.

Format	`no vlan acceptframe`
Mode	Interface Config

vlan ingressfilter

This command enables ingress filtering on an interface or range of interfaces. If ingress filtering is disabled, frames received with VLAN IDs that do not match the VLAN membership of the receiving interface are admitted and forwarded to ports that are members of that VLAN.

Default	disabled
Format	`vlan ingressfilter`
Mode	Interface Config

no vlan ingressfilter

This command disables ingress filtering. If ingress filtering is disabled, frames received with VLAN IDs that do not match the VLAN membership of the receiving interface are admitted and forwarded to ports that are members of that VLAN.

Format	`no vlan ingressfilter`
Mode	Interface Config

vlan makestatic

This command changes a dynamically created VLAN (created by GVRP registration) to a static VLAN (one that is permanently configured and defined). The ID is a valid VLAN identification number. VLAN range is 2-4093.

Format	`vlan makestatic` *`2-4093`*
Mode	VLAN Config

vlan name

This command changes the name of a VLAN. The name is an alphanumeric string of up to 32 characters, and the ID is a valid VLAN identification number. ID range is 1-4093.

Default	◆ VLAN ID 1 - default ◆ other VLANS - blank string
Format	`vlan name` *`1-4093 name`*
Mode	VLAN Config

no vlan name

This command sets the name of a VLAN to a blank string.

Format	`no vlan name` *`1-4093`*
Mode	VLAN Config

vlan participation

This command configures the degree of participation for a specific interface or range of interfaces in a VLAN. The ID is a valid VLAN identification number, and the interface is a valid interface number.

Format	`vlan participation {exclude | include | auto} 1-4093`
Mode	Interface Config

Participation options are:

Options	Definition
include	The interface is always a member of this VLAN. This is equivalent to registration fixed.
exclude	The interface is never a member of this VLAN. This is equivalent to registration forbidden.
auto	The interface is dynamically registered in this VLAN by GVRP and will not participate in this VLAN unless a join request is received on this interface. This is equivalent to registration normal.

vlan participation all

This command configures the degree of participation for all interfaces in a VLAN. The ID is a valid VLAN identification number.

Format	`vlan participation all {exclude | include | auto} 1-4093`
Mode	Global Config

You can use the following participation options:

Participation Options	Definition
include	The interface is always a member of this VLAN. This is equivalent to registration fixed.
exclude	The interface is never a member of this VLAN. This is equivalent to registration forbidden.

Participation Options	Definition
auto	The interface is dynamically registered in this VLAN by GVRP. The interface will not participate in this VLAN unless a join request is received on this interface. This is equivalent to registration normal.

vlan port acceptframe all

This command sets the frame acceptance mode for all interfaces.

Default	all
Format	`vlan port acceptframe all {vlanonly | admituntaggedonly |all}`
Mode	Global Config

The modes are defined as follows:

Mode	Definition
VLAN Only mode	Untagged frames or priority frames received on this interface are discarded.
Admit Untagged Only mode	VLAN-tagged and priority tagged frames received on this interface are discarded.
Admit All mode	Untagged frames or priority frames received on this interface are accepted and assigned the value of the interface VLAN ID for this port.

With either option, VLAN tagged frames are forwarded in accordance with the IEEE 802.1Q VLAN Specification.

no vlan port acceptframe all

This command sets the frame acceptance mode for all interfaces to Admit All. For Admit All mode, untagged frames or priority frames received on this interface are accepted and assigned the value of the interface VLAN ID for this port. With either option, VLAN tagged frames are forwarded in accordance with the IEEE 802.1Q VLAN Specification.

Format	`no vlan port acceptframe all`
Mode	Global Config

vlan port ingressfilter all

This command enables ingress filtering for all ports. If ingress filtering is disabled, frames received with VLAN IDs that do not match the VLAN membership of the receiving interface are admitted and forwarded to ports that are members of that VLAN.

Default	disabled
Format	`vlan port ingressfilter all`
Mode	Global Config

no vlan port ingressfilter all

This command disables ingress filtering for all ports. If ingress filtering is disabled, frames received with VLAN IDs that do not match the VLAN membership of the receiving interface are admitted and forwarded to ports that are members of that VLAN.

Format	`no vlan port ingressfilter all`
Mode	Global Config

vlan port pvid all

This command changes the VLAN ID for all interface.

Default	1
Format	`vlan port pvid all` *`1-4093`*
Mode	Global Config

no vlan port pvid all

This command sets the VLAN ID for all interfaces to 1.

Format	`no vlan port pvid all`

Mode	Global Config

vlan port tagging all

This command configures the tagging behavior for all interfaces in a VLAN to enabled. If tagging is enabled, traffic is transmitted as tagged frames. If tagging is disabled, traffic is transmitted as untagged frames. The ID is a valid VLAN identification number.

Format	`vlan port tagging all` *`1-4093`*
Mode	Global Config

no vlan port tagging all

This command configures the tagging behavior for all interfaces in a VLAN to disabled. If tagging is disabled, traffic is transmitted as untagged frames. The ID is a valid VLAN identification number.

Format	`no vlan port tagging all`
Mode	Global Config

vlan protocol group

This command adds protocol-based VLAN groups to the system. The *`groupid`* is a unique number from 1–128 that is used to identify the group in subsequent commands.

Format	`vlan protocol group` *`groupid`*
Mode	Global Config

vlan protocol group name

This command assigns a name to a protocol-based VLAN groups. The *groupname* variable can be a character string of 0 to 16 characters.

Format	`vlan protocol group name` *`groupid groupname`*
Mode	Global Config

no vlan protocol group name

This command removes the name from the group identified by *groupid*.

Format	no vlan protocol group name *groupid*
Mode	Global Config

vlan protocol group add protocol

This command adds the *protocol* to the protocol-based VLAN identified by *groupid*. A group may have more than one protocol associated with it. Each interface and protocol combination can only be associated with one group. If adding a protocol to a group causes any conflicts with interfaces currently associated with the group, this command fails and the protocol is not added to the group. The possible values for *protocol* are The possible values for *protocol-list* includes the keywords *ip, arp,* and *ipx* and hexadecimal or decimal values ranging from 0x0600 (1536) to 0xFFFF (65535). The protocol list can accept up to 16 protocols separated by a comma.

Default	none
Format	vlan protocol group add protocol *groupid ethertype protocol-list*
Mode	Global Config

no vlan protocol group add protocol

This command removes the protocols specified in the *protocol-list* from this protocol-based VLAN group that is identified by this *groupid*.

Format	no vlan protocol group add protocol *groupid ethertype protocol-list*
Mode	Global Config

protocol group

This command attaches a *vlanid* to the protocol-based VLAN identified by *groupid*. A group may only be associated with one VLAN at a time, however the VLAN association can be changed.

Default	none
Format	protocol group *groupid vlanid*

Mode	VLAN Config

no protocol group

This command removes the *vlanid* from this protocol-based VLAN group that is identified by this *groupid*.

Format	`no protocol group` *groupid vlanid*
Mode	VLAN Config

protocol vlan group

This command adds a physical interface or a range of interfaces to the protocol-based VLAN identified by *groupid*. You can associate multiple interfaces with a group, but you can only associate each interface and protocol combination with one group. If adding an interface to a group causes any conflicts with protocols currently associated with the group, this command fails and the interface(s) are not added to the group.

Default	none
Format	`protocol vlan group` *groupid*
Mode	Interface Config

no protocol vlan group

This command removes the interface from this protocol-based VLAN group that is identified by this *groupid*.

Format	`no protocol vlan group` *groupid*
Mode	Interface Config

protocol vlan group all

This command adds all physical interfaces to the protocol-based VLAN identified by *groupid*. You can associate multiple interfaces with a group, but you can only associate each interface and protocol combination with one group. If adding an interface to a group causes any conflicts with protocols currently associated with the group, this command will fail and the interface(s) will not be added to the group.

Default	none
Format	`protocol vlan group all` *`groupid`*
Mode	Global Config

no protocol vlan group all

This command removes all interfaces from this protocol-based VLAN group that is identified by this *`groupid`*.

Format	`no protocol vlan group all` *`groupid`*
Mode	Global Config

show port protocol

This command displays the Protocol-Based VLAN information for either the entire system, or for the indicated group.

Format	`show port protocol {`*`groupid`* `| all}`
Mode	Privileged EXEC

Term	Definition
Group Name	The group name of an entry in the Protocol-based VLAN table.
Group ID	The group identifier of the protocol group.
VLAN	The VLAN associated with this Protocol Group.
Protocol(s)	The type of protocol(s) for this group.
Interface(s)	Lists the slot/port interface(s) that are associated with this Protocol Group.

vlan pvid

This command changes the VLAN ID on an interface or range of interfaces.

Default	1
Format	`vlan pvid 1-4093`
Mode	Interface Config Interface Range Config

no vlan pvid

This command sets the VLAN ID on an interface or range of interfaces to 1.

Format	`no vlan pvid`
Mode	Interface Config

vlan tagging

This command configures the tagging behavior for a specific interface or range of interfaces in a VLAN to enabled. If tagging is enabled, traffic is transmitted as tagged frames. If tagging is disabled, traffic is transmitted as untagged frames. The ID is a valid VLAN identification number.

Format	`vlan tagging 1-4093`
Mode	◆ Interface Config

no vlan tagging

This command configures the tagging behavior for a specific interface or range of interfaces in a VLAN to disabled. If tagging is disabled, traffic is transmitted as untagged frames. The ID is a valid VLAN identification number.

Format	`no vlan tagging 1-4093`
Mode	◆ Interface Config

vlan association subnet

This command associates a VLAN to a specific IP-subnet.

Format	`vlan association subnet ipaddr netmask vlanid`
Mode	VLAN Config

no vlan association subnet

This command removes association of a specific IP-subnet to a VLAN.

Format	`no vlan association subnet` *`ipaddr netmask`*
Mode	VLAN Config

vlan association mac

This command associates a MAC address to a VLAN.

Format	`vlan association mac` *`macaddr vlanid`*
Mode	VLAN database

no vlan association mac

This command removes the association of a MAC address to a VLAN.

Format	`no vlan association mac` *`macaddr`*
Mode	VLAN database

remote-span

This command identifies the VLAN as the RSPAN VLAN.

Default	`None`
Format	`remote-span`
Mode	VLAN configuration

show vlan

This command displays information about the configured private VLANs, including primary and secondary VLAN IDs, type (community, isolated, or primary) and the ports which belong to a private VLAN.

Format	`show vlan {`*`vlanid`*`|private-vlan [`*`type`*`]}`
Mode	◆ Privileged EXEC ◆ User EXEC

Term	Definition
Primary	Primary VLAN identifier. The range of the VLAN ID is 1 to 4093.
Secondary	Secondary VLAN identifier.
Type	Secondary VLAN type (community, isolated, or primary).
Ports	Ports which are associated with a private VLAN.
VLAN ID	The VLAN identifier (VID) associated with each VLAN. The range of the VLAN ID is 1 to 4093.
VLAN Name	A string associated with this VLAN as a convenience. It can be up to 32 alphanumeric characters long, including blanks. The default is blank. VLAN ID 1 always has a name of **Default**. This field is optional.
VLAN Type	Type of VLAN, which can be Default (VLAN ID = 1) or static (one that is configured and permanently defined), or Dynamic. A dynamic VLAN can be created by GVRP registration or during the 802.1X authentication process (DOT1X) if a RADIUS-assigned VLAN does not exist on the switch.
Interface	slot/port. It is possible to set the parameters for all ports by using the selectors on the top line.

Term	Definition
Current	The degree of participation of this port in this VLAN. The permissible values are: ◆ **Include** - This port is always a member of this VLAN. This is equivalent to registration fixed in the IEEE 802.1Q standard. ◆ **Exclude** - This port is never a member of this VLAN. This is equivalent to registration forbidden in the IEEE 802.1Q standard. ◆ **Autodetect** - To allow the port to be dynamically registered in this VLAN via GVRP. The port will not participate in this VLAN unless a join request is received on this port. This is equivalent to registration normal in the IEEE 802.1Q standard.
Configured	The configured degree of participation of this port in this VLAN. The permissible values are: ◆ **Include** - This port is always a member of this VLAN. This is equivalent to registration fixed in the IEEE 802.1Q standard. ◆ **Exclude** - This port is never a member of this VLAN. This is equivalent to registration forbidden in the IEEE 802.1Q standard. ◆ **Autodetect** - To allow the port to be dynamically registered in this VLAN via GVRP. The port will not participate in this VLAN unless a join request is received on this port. This is equivalent to registration normal in the IEEE 802.1Q standard.
Tagging	The tagging behavior for this port in this VLAN. ◆ **Tagged** - Transmit traffic for this VLAN as tagged frames. ◆ **Untagged** - Transmit traffic for this VLAN as untagged frames.

show vlan brief This command displays a list of all configured VLANs.

Format	`show vlan brief`
Mode	◆ Privileged EXEC ◆ User EXEC

Term	Definition
VLAN ID	There is a VLAN Identifier (vlanid) associated with each VLAN. The range of the VLAN ID is 1 to 4093.
VLAN Name	A string associated with this VLAN as a convenience. It can be up to 32 alphanumeric characters long, including blanks. The default is blank. VLAN ID 1 always has a name of “Default.” This field is optional.
VLAN Type	Type of VLAN, which can be Default (VLAN ID = 1) or static (one that is configured and permanently defined), or a Dynamic (one that is created by GVRP registration).

show vlan port

This command displays VLAN port information.

Format	`show vlan port {slot/port | all}`
Mode	◆ Privileged EXEC ◆ User EXEC

Term	Definition
Interface	slot/port It is possible to set the parameters for all ports by using the selectors on the top line.
Port VLAN ID Configured	The VLAN ID that this port will assign to untagged frames or priority tagged frames received on this port. The value must be for an existing VLAN. The factory default is 1.

Term	Definition
Port VLAN ID Current	The current VLAN ID that this port assigns to untagged frames or priority tagged frames received on this port. The factory default is 1.
Acceptable Frame Types	The types of frames that may be received on this port. The options are 'VLAN only' and 'Admit All'. When set to 'VLAN only', untagged frames or priority tagged frames received on this port are discarded. When set to 'Admit All', untagged frames or priority tagged frames received on this port are accepted and assigned the value of the Port VLAN ID for this port. With either option, VLAN tagged frames are forwarded in accordance to the 802.1Q VLAN specification.
Ingress Filtering Configured	May be enabled or disabled. When enabled, the frame is discarded if this port is not a member of the VLAN with which this frame is associated. In a tagged frame, the VLAN is identified by the VLAN ID in the tag. In an untagged frame, the VLAN is the Port VLAN ID specified for the port that received this frame. When disabled, all frames are forwarded in accordance with the 802.1Q VLAN bridge specification. The factory default is disabled.
Ingress Filtering Current	Shows the current ingress filtering configuration.
GVRP	May be enabled or disabled.
Default Priority	The 802.1p priority assigned to tagged packets arriving on the port.
Protected Port	Specifies if this is a protected port. If False, it is not a protected port; If true, it is.
Switchport mode	The current switchport mode for the port.
Operating parameters	The operating parameters for the port, including the VLAN, name, egress rule, and type.

Term	Definition
Static configuration	The static configuration for the port, including the VLAN, name, and egress rule.
Forbidden VLANs	The forbidden VLAN configuration for the port, including the VLAN and name.

show vlan association subnet

This command displays the VLAN associated with a specific configured IP-Address and net mask. If no IP address and net mask are specified, the VLAN associations of all the configured IP-subnets are displayed.

Format	`show vlan association subnet [`*`ipaddr netmask`*`]`
Mode	Privileged EXEC

Term	Definition
IP Address	The IP address assigned to each interface.
Net Mask	The subnet mask.
VLAN ID	There is a VLAN Identifier (VID) associated with each VLAN.

show vlan association mac

This command displays the VLAN associated with a specific configured MAC address. If no MAC address is specified, the VLAN associations of all the configured MAC addresses are displayed.

Format	`show vlan association mac` *`[macaddr]`*
Mode	Privileged EXEC

Term	Definition
Mac Address	A MAC address for which the switch has forwarding and or filtering information. The format is 6 or 8 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB. In an IVL system the MAC address will be displayed as 8 bytes.
VLAN ID	There is a VLAN Identifier (VID) associated with each VLAN.

Double VLAN Commands

This section describes the commands you use to configure double VLAN (DVLAN). Double VLAN tagging is a way to pass VLAN traffic from one customer domain to another through a Metro Core in a simple and cost effective manner. The additional tag on the traffic helps differentiate between customers in the MAN while preserving the VLAN identification of the individual customers when they enter their own IEEE 802.1Q domain.

dvlan-tunnel ethertype

This command configures the ethertype for the switch. The two-byte hex ethertype is used as the first 16 bits of the DVLAN tag. The ethertype may have the values of *802.1Q*, *vman*, or *custom*. If the ethertype has an optional value of *custom*, then it is a custom tunnel value, and ethertype must be set to a value in the range of 1 to 65535.

Default	vman
Format	`dvlan-tunnel ethertype {802.1Q | vman | custom` *`1-65535`*`}`
Mode	Global Config

Parameter	Description
802.1Q	Configure the ethertype as 0x8100.
custom	Configure the value of the custom tag in the range from 1to 65535.
vman	Represents the commonly used value of 0x88A8.

no dvlan-tunnel ethertype

This command removes the ethertype value for the switch.

Format	`no dvlan-tunnel ethertype`
Mode	Global Config

mode dot1q-tunnel

This command is used to enable Double VLAN Tunneling on the specified interface.

Default	disabled
Format	`mode dot1q-tunnel`
Mode	Interface Config

no mode dot1q-tunnel

This command is used to disable Double VLAN Tunneling on the specified interface. By default, Double VLAN Tunneling is disabled.

Format	`no mode dot1q-tunnel`
Mode	Interface Config

mode dvlan-tunnel

Use this command to enable Double VLAN Tunneling on the specified interface.

Note

When you use the `mode dvlan-tunnel` command on an interface, it becomes a service provider port. Ports that do not have double VLAN tunneling enabled are customer ports.

Default	disabled
Format	`mode dvlan-tunnel`
Mode	Interface Config

no mode dvlan-tunnel

This command is used to disable Double VLAN Tunneling on the specified interface. By default, Double VLAN Tunneling is disabled.

Format	`no mode dvlan-tunnel`
Mode	Interface Config

show dot1q-tunnel

Use this command without the optional parameters to display all interfaces enabled for Double VLAN Tunneling. Use the optional parameters to display detailed information about Double VLAN Tunneling for the specified interface or all interfaces.

Format	`show dot1q-tunnel [interface {slot/port | all}]`
Mode	◆ Privileged EXEC ◆ User EXEC

Term	Definition
Interface	slot/port
Mode	The administrative mode through which Double VLAN Tunneling can be enabled or disabled. The default value for this field is disabled.
EtherType	A 2-byte hex EtherType to be used as the first 16 bits of the DVLAN tunnel. There are three different EtherType tags. The first is 802.1Q, which represents the commonly used value of 0x8100. The second is vMAN, which represents the commonly used value of 0x88A8. If EtherType is not one of these two values, then it is a custom tunnel value, representing any value in the range of 1 to 65535.

show dvlan-tunnel

Use this command without the optional parameters to display all interfaces enabled for Double VLAN Tunneling. Use the optional parameters to display detailed information about Double VLAN Tunneling for the specified interface or all interfaces.

Format	`show dvlan-tunnel [interface {slot/port|all|lag` *`lag-intf-num`*`}]`
Mode	◆ Privileged EXEC ◆ User EXEC

Term	Definition
Interface	slot/port
LAG	Instead of slot/port, *lag* lag-intf-num can be used as an alternate way to specify the LAG interface. lag lag-intf-num can also be used to specify the LAG interface where lag-intf-num is the LAG port number.
Mode	The administrative mode through which Double VLAN Tunneling can be enabled or disabled. The default value for this field is disabled.
EtherType	A 2-byte hex EtherType to be used as the first 16 bits of the DVLAN tunnel. There are three different EtherType tags. The first is 802.1Q, which represents the commonly used value of 0x8100. The second is vMAN, which represents the commonly used value of 0x88A8. If EtherType is not one of these two values, then it is a custom tunnel value, representing any value in the range of 1 to 65535.

The following shows examples of the CLI display output for the commands.

```
(CN1610) #show dvlan-tunnel

Primary TPID.................................. 0x8100
Secondary TPIDs Configured.....................
Interfaces Enabled for DVLAN Tunneling......... None

(CN1610)#show dvlan-tunnel interface 0/1

Interface Mode    EtherType
--------- ------- ------------
0/1     Disable 0x88a8
```

Private VLAN Commands

This section describes the commands you use for private VLANs. Private VLANs provides Layer 2 isolation between ports that share the same broadcast domain. In other words, it allows a VLAN broadcast domain to be partitioned into smaller point-to-multipoint subdomains. The ports participating in a private VLAN can be located anywhere in the Layer 2 network.

switchport private-vlan

This command defines a private-VLAN association for an isolated or community port or a mapping for a promiscuous port.

Format	`switchport private-vlan {host-association` *`primary-vlan-id secondary-vlan-id`* `| mapping` *`primary-vlan-id`* `{add | remove}` *`secondary-vlan-list`*`}`
Mode	Interface Config

Parameter	Description
host-association	Defines the VLAN association for community or host ports.
mapping	Defines the private VLAN mapping for promiscuous ports.
primary-vlan-id	Primary VLAN ID of a private VLAN.
secondary-vlan-id	Secondary (isolated or community) VLAN ID of a private VLAN.
add	Associates the secondary VLAN with the primary one.
remove	Deletes the secondary VLANs from the primary VLAN association.
secondary-vlan-list	A list of secondary VLANs to be mapped to a primary VLAN.

no switchport private-vlan

This command removes the private-VLAN association or mapping from the port.

Format	`no switchport private-vlan {host-association|mapping}`
Mode	Interface Config

switchport mode private-vlan

This command configures a port as a promiscuous or host private VLAN port. Note that the properties of each mode can be configured even when the switch is not in that mode. However, they will only be applicable once the switch is in that particular mode.

Default	`general`
Format	`switchport mode private-vlan {host|promiscuous}`
Mode	Interface Config

Parameter	Description
host	Configures an interface as a private VLAN host port. It can be either isolated or community port depending on the secondary VLAN it is associated with.
promiscuous	Configures an interface as a private VLAN promiscuous port. The promiscuous ports are members of the primary VLAN.

no switchport mode private-vlan

This command removes the private-VLAN association or mapping from the port.

Format	`no switchport mode private-vlan`
Mode	Interface Config

private-vlan

This command configures the private VLANs and configures the association between the primary private VLAN and secondary VLANs.

Format	`private-vlan {association [add|remove] secondary-vlan-list|community|isolated|primary}`
Mode	VLAN Config

Parameter	Description
association	Associates the primary and secondary VLAN.
secondary-vlan-list	A list of secondary VLANs to be mapped to a primary VLAN.
community	Designates a VLAN as a community VLAN.
isolated	Designates a VLAN as the isolated VLAN.
primary	Designates a VLAN as the primary VLAN.

no private-vlan This command restores normal VLAN configuration.

Format	`no private-vlan {association}`
Mode	VLAN Config

Switch Ports

This section describes the commands used for switch port mode.

switchport mode

Use this command to configure the mode of a switch port as access, trunk or general.

In Trunk mode, the port becomes a member of all VLANs on switch unless specified in the allowed list in the `switchport trunk allowed vlan` command. The PVID of the port is set to the Native VLAN as specified in the `switchport trunk native vlan` command. It means that trunk ports accept both tagged and untagged packets, where untagged packets are processed on the native VLAN and tagged packets are processed on the VLAN ID contained in the packet. MAC learning is performed on both tagged and untagged packets. Tagged packets received with a VLAN ID of which the port is not a member are discarded and MAC learning is not performed. The Trunk ports always transmit packets untagged on native VLAN.

In Access mode, the port becomes a member of only one VLAN. The port sends and receives untagged traffic. It can also receive tagged traffic.The ingress filtering is enabled on port. It means that when the VLAN ID of received packet is not identical to Access VLAN ID, the packet is discarded.

In General mode, the user can perform custom configuration of VLAN membership, PVID, tagging, ingress filtering etc. This is legacy FASTPATH behavior of switch port configuration. Legacy FASTPATH CLI commands are used to configure port in general mode.

Default	General mode
Format	`switchport mode {access | trunk | general}`
Mode	Interface Config

no switchport mode

This command resets the switch port mode to its default value.

Format	`no switchport mode`
Mode	Interface Config

switchport trunk allowed vlan

Use this command to configure the list of allowed VLANs that can receive and send traffic on this interface in tagged format when in trunking mode. The default is all.

The VLANs list can be modified using the add or remove options or replaced with another list using the vlan-list, all, or except options. If all is choosen, all VLANs are added to the list of allowed vlan. The except option provides an exclusion list.

Trunk ports accept tagged packets, where tagged packets are processed on the VLAN ID contained in the packet, if this VLAN is in the allowed VLAN list. Tagged packets received with a VLAN ID to which the port is not a member are discarded and MAC learning is not performed. If a VLAN is added to the system after a port is set to the Trunk mode and it is in the allowed VLAN list, this VLAN is assigned to this port automatically.

Default	All
Format	`switchport trunk allowed vlan {`*`vlan-list`*` | all | {add `*`vlan-list`*`} | {remove `*`vlan-list`*`} | {except `*`vlan-list`*` }}`
Mode	Interface Config

Parameter	Description
all	Specifies all VLANs from 1 to 4093. This keyword is not allowed on commands that do not permit all VLANs in the list to be set at the same time.
add	Adds the defined list of VLANs to those currently set instead of replacing the list.
remove	Removes the defined list of VLANs from those currently set instead of replacing the list. Valid IDs are from 1 to 4093; extended-range VLAN IDs of the form X-Y or X,Y,Z are valid in this command.
except	Lists the VLANs that should be calculated by inverting the defined list of VLANs. (VLANs are added except the ones specified.)

Parameter	Description
vlan-list	Either a single VLAN number from 1 to 4093 or a continuous range of VLANs described by two VLAN numbers, the lesser one first, separated by a hyphen.

no switchport trunk allowed vlan

This command resets the list of allowed VLANs on the trunk port to its default value.

Format	`no switchport trunk allowed vlan`
Mode	Interface Config

switchport trunk native vlan

Use this command to configure the Trunk port Native VLAN (PVID) parameter. Any ingress untagged packets on the port are tagged with the value of Native VLAN. Native VLAN must be in the allowed VLAN list for tagging of received untagged packets. Otherwise, untagged packets are discarded. Packets marked with Native VLAN are transmitted untagged from Trunk port. The default is 1.

Default	1 (Default VLAN)
Format	`switchport trunk native vlan` *`vlan-id`*
Mode	Interface Config

no switchport trunk native vlan

Use this command to reset the switch port trunk mode native VLAN to its default value.

Format	`no switchport trunk native vlan`
Mode	Interface Config

switchport access vlan

Use this command to configure the VLAN on the Access port. Only one VLAN can be assigned to the Access port. Access ports are members of VLAN 1 by default. Access ports may be assigned to a VLAN other than VLAN 1. Removing

the Access VLAN on the switch makes the Access port a member of VLAN 1. Configuring an Access port to be a member of a VLAN that does not exist results in an error and does not change the configuration.

Default	1 (Default VLAN)
Format	`switchport access vlan` *`vlan-id`*
Mode	Interface Config

no switchport access vlan

This command resets the switch port access mode VALN to its default value.

Format	`no switchport access vlan`
Mode	Interface Config

show interfaces switchport

Use this command to display the switchport status for all interfaces or a specified interface.

Format	`show interfaces switchport slot/port`
Mode	Privileged EXEC

```
(CN1610) #show interfaces switchport 1/0/1

Port: 1/0/1
VLAN Membership Mode: General
Access Mode VLAN: 1 (default)
General Mode PVID: 1 (default)
General Mode Ingress Filtering: Disabled
General Mode Acceptable Frame Type: Admit all
General Mode Dynamically Added VLANs:
General Mode Untagged VLANs: 1
General Mode Tagged VLANs:
General Mode Forbidden VLANs:
Trunking Mode Native VLAN: 1 (default)
Trunking Mode Native VLAN tagging: Disable
Trunking Mode VLANs Enabled: All
Protected Port: False
```

```
(CN1610) #show interfaces switchport

Port: 1/0/1
VLAN Membership Mode: General
Access Mode VLAN: 1 (default)
General Mode PVID: 1 (default)
General Mode Ingress Filtering: Disabled
General Mode Acceptable Frame Type: Admit all
General Mode Dynamically Added VLANs:
General Mode Untagged VLANs: 1
General Mode Tagged VLANs:
General Mode Forbidden VLANs:
Trunking Mode Native VLAN: 1 (default)
Trunking Mode Native VLAN tagging: Disable
Trunking Mode VLANs Enabled: All
Protected Port: False
```

show interfaces switchport

Use this command to display the Switchport configuration for a selected mode per interface. If the interface is not specified, the configuration for all interfaces is displayed.

Format	`show interfaces switchport {access | trunk | general} [slot/port]`
Mode	Privileged EXEC

```
Switching) # show interfaces switchport access 1/0/1

Intf      PVID
--------- ----
1/0/1     1


(Switching) # show interfaces switchport trunk 1/0/6

Intf      PVID  Allowed Vlans List
--------- ----- -------------------
1/0/6     1     All


(Switching) # show interfaces switchport general 1/0/5

Intf     PVID  Ingress    Acceptable  Untagged  Tagged   Forbidden
Dynamic
```

```
                Filtering   Frame Type  Vlans     Vlans    Vlans
Vlans
--------- ----- ---------- ----------  --------- --------- --------
- ---------
1/0/5     1     Enabled    Admit All   7         10-50,55  9,100-200
88,96


(Switching) # show interfaces switchport general

Intf      PVID  Ingress    Acceptable  Untagged  Tagged   Forbidden
Dynamic
                Filtering   Frame Type  Vlans     Vlans    Vlans
Vlans
--------- ----- ---------- ----------  --------- --------- --------
- ---------
1/0/1     1     Enabled    Admit All   1,4-7     30-40,55  3,100-200
88,96
1/0/2     1     Disabled   Admit All   1         30-40,55  none
none
..
```

Voice VLAN Commands

This section describes the commands you use for Voice VLAN. Voice VLAN enables switch ports to carry voice traffic with defined priority so as to enable separation of voice and data traffic coming onto the port. The benefits of using Voice VLAN is to ensure that the sound quality of an IP phone could be safeguarded from deteriorating when the data traffic on the port is high.

Also the inherent isolation provided by VLANs ensures that inter-VLAN traffic is under management control and that network- attached clients cannot initiate a direct attack on voice components. QoS-based on IEEE 802.1P class of service (CoS) uses classification and scheduling to sent network traffic from the switch in a predictable manner. The system uses the source MAC of the traffic traveling through the port to identify the IP phone data flow.

voice vlan (Global Config)

Use this command to enable the Voice VLAN capability on the switch.

Default	disabled
Format	`voice vlan`
Mode	Global Config

no voice vlan (Global Config)

Use this command to disable the Voice VLAN capability on the switch.

Format	`no voice vlan`
Mode	Global Config

voice vlan (Interface Config)

Use this command to enable the Voice VLAN capability on the interface or range of interfaces.

Default	disabled
Format	`voice vlan {vlanid` *`id`* `| dot1p` *`priority`* `| none | untagged}`
Mode	Interface Config

You can configure Voice VLAN in one of four different ways:

Parameter	Description
vlan-id	Configure the IP phone to forward all voice traffic through the specified VLAN. Valid VLAN ID's are from 1 to 4093 (the max supported by the platform).
dot1p	Configure the IP phone to use 802.1p priority tagging for voice traffic and to use the default native VLAN (VLAN 0) to carry all traffic. Valid *priority* range is 0 to 7.
none	Allow the IP phone to use its own configuration to send untagged voice traffic.
untagged	Configure the phone to send untagged voice traffic.

no voice vlan (Interface Config)

Use this command to disable the Voice VLAN capability on the interface.

Format	`no voice vlan`
Mode	Interface Config

voice vlan data priority

Use this command to either trust or untrust the data traffic arriving on the Voice VLAN interface or range of interfaces being configured.

Default	trust
Format	`voice vlan data priority {untrust | trust}`
Mode	Interface Config

show voice vlan

Format	`show voice vlan [interface {`*`unit/slot/port`*` | all}]`
Mode	Privileged EXEC

When the `interface` parameter is not specified, only the global mode of the Voice VLAN is displayed.

Term	Definition
Administrative Mode	The Global Voice VLAN mode.

When the `interface` is specified:

Term	Definition
Voice VLAN Mode	The admin mode of the Voice VLAN on the interface.
Voice VLAN ID	The Voice VLAN ID
Voice VLAN Priority	The do1p priority for the Voice VLAN on the port.
Voice VLAN Untagged	The tagging option for the Voice VLAN traffic.
Voice VLAN CoS Override	The Override option for the voice traffic arriving on the port.
Voice VLAN Status	The operational status of Voice VLAN on the port.

Provisioning (IEEE 802.1p) Commands

This section describes the commands you use to configure provisioning (IEEE 802.1p,) which allows you to prioritize ports.

vlan port priority all

This command configures the port priority assigned for untagged packets for all ports presently plugged into the device. The range for the priority is 0-7. Any subsequent per port configuration will override this configuration setting.

Format	`vlan port priority all` *priority*
Mode	Global Config

vlan priority

This command configures the default 802.1p port priority assigned for untagged packets for a specific interface. The range for the priority is 0–7.

Default	0
Format	`vlan priority` *priority*
Mode	Interface Config

Asymmetric Flow Control

When in asymmetric flow control mode, the switch responds to PAUSE frames received from a peer by stopping packet transmission, but the switch does not initiate MAC control PAUSE frames.

When you configure the switch in asymmetric flow control (or no flow control mode), the device is placed in egress drop mode. Egress drop mode maximizes the throughput of the system at the expense of packet loss in a heavily congested system, and this mode avoids head-of-line blocking.

flowcontrol {symmetric|asymmetric}

Use this command to enable or disable the symmetric or asymmetric flow control on the switch. Asymmetric here means that **Tx Pause** can never be enabled. Only **Rx Pause** can be enabled.

Default	Flow control is disabled.
Format	`flowcontrol {symmetric|asymmetric}`
Mode	Global Config

no flowcontrol {symmetric|asymmetric}

Use the **no** form of this command to disable symmetric or asymmetric flow control.

Format	`no flowcontrol {symmetric|asymmetric}`
Mode	Global Config

flowcontrol

Use this command to enable or disable the symmetric flow control on the switch.

Default	Flow control is disabled.
Format	`flowcontrol`
Mode	Global Config

no flowcontrol

Use the **no** form of this command to disable the symmetric flow control.

Format	no flowcontrol
Mode	Global Config

show flowcontrol

Use this command to display the IEEE 802.3 Annex 31B flow control settings and status for a specific interface or all interfaces. The command also displays 802.3 Tx and Rx pause counts. Priority Flow Control frames counts are not displayed. If the port is enabled for priority flow control, operational flow control status is displayed as **Inactive**.

Format	show flowcontrol [slot/port]
Mode	Privileged EXEC

The following shows example CLI display output for the command.

```
(CN1610)#show flowcontrol

Admin Flow Control: Symmetric

Port    Flow Control    RxPause    TxPause
        Oper
------  ------------    --------   ---------
0/1     Active          310        611

0/2     Inactive        0           0
```

The following shows example CLI display output for the command.

```
(CN1610)#show flowcontrol interface 0/1

Admin Flow Control: Symmetric

Port       Flow Control  RxPause      TxPause
           Oper
---------  -------       --------     -------
0/1        Active        310          611
```

Protected Ports Commands

This section describes commands you use to configure and view protected ports on a switch. Protected ports do not forward traffic to each other, even if they are on the same VLAN. However, protected ports can forward traffic to all unprotected ports in their group. Unprotected ports can forward traffic to both protected and unprotected ports. Ports are unprotected by default.

If an interface is configured as a protected port, and you add that interface to a Port Channel or Link Aggregation Group (LAG), the protected port status becomes operationally disabled on the interface, and the interface follows the configuration of the LAG port. However, the protected port configuration for the interface remains unchanged. Once the interface is no longer a member of a LAG, the current configuration for that interface automatically becomes effective.

switchport protected (Global Config)

Use this command to create a protected port group. The *groupid* parameter identifies the set of protected ports. Use the `name` *name* pair to assign a name to the protected port group. The name can be up to 32 alphanumeric characters long, including blanks. The default is blank.

Note
Port protection occurs within a single switch. Protected port configuration does not affect traffic between ports on two different switches. No traffic forwarding is possible between two protected ports.

Default	unprotected
Format	`switchport protected` *groupid* `name` *name*
Mode	Global Config

no switchport protected (Global Config)

Use this command to remove a protected port group. The *groupid* parameter identifies the set of protected ports. The `name` keyword specifies the name to remove from the group.

Format	`no switchport protected` *groupid* `name`
Mode	Global Config

switchport protected (Interface Config)

Use this command to add an interface to a protected port group. The *groupid* parameter identifies the set of protected ports to which this interface is assigned. You can only configure an interface as protected in one group.

Note

Port protection occurs within a single switch. Protected port configuration does not affect traffic between ports on two different switches. No traffic forwarding is possible between two protected ports.

Default	unprotected
Format	`switchport protected` *groupid*
Mode	Interface Config

no switchport protected (Interface Config)

Use this command to configure a port as unprotected. The *groupid* parameter identifies the set of protected ports to which this interface is assigned.

Format	`no switchport protected` *groupid*
Mode	Interface Config

show switchport protected

This command displays the status of all the interfaces, including protected and unprotected interfaces.

Format	`show switchport protected` *groupid*
Mode	◆ Privileged EXEC ◆ User EXEC

Term	Definition
Group ID	The number that identifies the protected port group.
Name	An optional name of the protected port group. The name can be up to 32 alphanumeric characters long, including blanks. The default is blank.

Term	Definition
List of Physical Ports	List of ports, which are configured as protected for the group identified with *groupid*. If no port is configured as protected for this group, this field is blank.

show interfaces switchport

This command displays the status of the interface (protected/unprotected) under the groupid.

Format	`show interfaces switchport slot/port` *groupid*
Mode	◆ Privileged EXEC ◆ User EXEC

Term	Definition
Name	A string associated with this group as a convenience. It can be up to 32 alphanumeric characters long, including blanks. The default is blank. This field is optional.
Protected	Indicates whether the interface is protected or not. It shows TRUE or FALSE. If the group is a multiple groups then it shows TRUE in Group *groupid*.

GARP Commands

This section describes the commands you use to configure Generic Attribute Registration Protocol (GARP) and view GARP status. The commands in this section affect both GARP VLAN Registration Protocol (GVRP) and GARP Multicast Registration Protocol (GMRP). GARP is a protocol that allows client stations to register with the switch for membership in VLANS (by using GVMP) or multicast groups (by using GVMP).

set garp timer join

This command sets the GVRP join time per GARP for one interface, a range of interfaces, or all interfaces. Join time is the interval between the transmission of GARP Protocol Data Units (PDUs) registering (or reregistering) membership for a VLAN or multicast group. This command has an effect only when GVRP is enabled. The time is from 10 to 100 (centiseconds). The value 20 centiseconds is 0.2 seconds.

Default	20
Format	`set garp timer join` *`10-100`*
Mode	◆ Interface Config ◆ Global Config

no set garp timer join

This command sets the GVRP join time to the default and only has an effect when GVRP is enabled.

Format	`no set garp timer join`
Mode	◆ Interface Config ◆ Global Config

set garp timer leave

This command sets the GVRP leave time for one interface, a range of interfaces, or all interfaces or all ports and only has an effect when GVRP is enabled. Leave time is the time to wait after receiving an unregister request for a VLAN or a multicast group before deleting the VLAN entry. This can be considered a buffer time for another station to assert registration for the same attribute in order to

maintain uninterrupted service. The leave time is 20 to 600 (centiseconds). The value 60 centiseconds is 0.6 seconds. The leave time must be greater than or equal to three times the join time.

Default	60
Format	`set garp timer leave` *`20-600`*
Mode	◆ Interface Config ◆ Global Config

no set garp timer leave

This command sets the GVRP leave time on all ports or a single port to the default and only has an effect when GVRP is enabled.

Format	`no set garp timer leave`
Mode	◆ Interface Config ◆ Global Config

set garp timer leaveall

This command sets how frequently Leave All PDUs are generated. A Leave All PDU indicates that all registrations will be unregistered. Participants would need to rejoin in order to maintain registration. The value applies per port and per GARP participation. The time may range from 200 to 6000 (centiseconds). The value 1000 centiseconds is 10 seconds. You can use this command on all ports (Global Config mode), or on a single port or a range of ports (Interface Config mode) and it only has an effect only when GVRP is enabled. The leave all time must be greater than the leave time.

Default	1000
Format	`set garp timer leaveall` *`200-6000`*
Mode	◆ Interface Config ◆ Global Config

no set garp timer leaveall

This command sets how frequently Leave All PDUs are generated the default and only has an effect when GVRP is enabled.

Format	`no set garp timer leaveall`
Mode	◆ Interface Config ◆ Global Config

show garp

This command displays GARP information.

Format	`show garp`
Mode	◆ Privileged EXEC ◆ User EXEC

Term	Definition
GMRP Admin Mode	The administrative mode of GARP Multicast Registration Protocol (GMRP) for the system.
GVRP Admin Mode	The administrative mode of GARP VLAN Registration Protocol (GVRP) for the system.

GVRP Commands

This section describes the commands you use to configure and view GARP VLAN Registration Protocol (GVRP) information. GVRP-enabled switches exchange VLAN configuration information, which allows GVRP to provide dynamic VLAN creation on trunk ports and automatic VLAN pruning.

Note
If GVRP is disabled, the system does not forward GVRP messages.

set gvrp adminmode

This command enables GVRP on the system.

Default	disabled
Format	`set gvrp adminmode`
Mode	Privileged EXEC

no set gvrp adminmode

This command disables GVRP.

Format	`no set gvrp adminmode`
Mode	Privileged EXEC

set gvrp interfacemode

This command enables GVRP on a single port (Interface Config mode), a range of ports (Interface Range mode), or all ports (Global Config mode).

Default	disabled
Format	`set gvrp interfacemode`
Mode	◆ Interface Config ◆ Interface Range ◆ Global Config

no set gvrp interfacemode

This command disables GVRP on a single port (Interface Config mode) or all ports (Global Config mode). If GVRP is disabled, Join Time, Leave Time and Leave All Time have no effect.

Format	`no set gvrp interfacemode`
Mode	◆ Interface Config ◆ Global Config

show gvrp configuration

This command displays Generic Attributes Registration Protocol (GARP) information for one or all interfaces.

Format	`show gvrp configuration {slot/port | all}`
Mode	◆ Privileged EXEC ◆ User EXEC

Term	Definition
Interface	slot/port
Join Timer	The interval between the transmission of GARP PDUs registering (or reregistering) membership for an attribute. Current attributes are a VLAN or multicast group. There is an instance of this timer on a per-Port, per-GARP participant basis. Permissible values are 10 to 100 centiseconds (0.1 to 1.0 seconds). The factory default is 20 centiseconds (0.2 seconds). The finest granularity of specification is one centisecond (0.01 seconds).

Term	Definition
Leave Timer	The period of time to wait after receiving an unregister request for an attribute before deleting the attribute. Current attributes are a VLAN or multicast group. This may be considered a buffer time for another station to assert registration for the same attribute in order to maintain uninterrupted service. There is an instance of this timer on a per-Port, per-GARP participant basis. Permissible values are 20 to 600 centiseconds (0.2 to 6.0 seconds). The factory default is 60 centiseconds (0.6 seconds).
LeaveAll Timer	This Leave All Time controls how frequently LeaveAll PDUs are generated. A LeaveAll PDU indicates that all registrations will shortly be deregistered. Participants will need to rejoin in order to maintain registration. There is an instance of this timer on a per-Port, per-GARP participant basis. The Leave All Period Timer is set to a random value in the range of LeaveAllTime to 1.5*LeaveAllTime. Permissible values are 200 to 6000 centiseconds (2 to 60 seconds). The factory default is 1000 centiseconds (10 seconds).
Port GMRP Mode	The GMRP administrative mode for the port, which is enabled or disabled (default). If this parameter is disabled, Join Time, Leave Time and Leave All Time have no effect.

GMRP Commands

This section describes the commands you use to configure and view GARP Multicast Registration Protocol (GMRP) information. Like IGMP snooping, GMRP helps control the flooding of multicast packets.GMRP-enabled switches dynamically register and de-register group membership information with the MAC networking devices attached to the same segment. GMRP also allows group membership information to propagate across all networking devices in the bridged LAN that support Extended Filtering Services.

Note
If GMRP is disabled, the system does not forward GMRP messages.

set gmrp adminmode

This command enables GARP Multicast Registration Protocol (GMRP) on the system.

Default	disabled
Format	`set gmrp adminmode`
Mode	Privileged EXEC

no set gmrp adminmode

This command disables GARP Multicast Registration Protocol (GMRP) on the system.

Format	`no set gmrp adminmode`
Mode	Privileged EXEC

set gmrp interfacemode

This command enables GARP Multicast Registration Protocol on a single interface (Interface Config mode), a range of interfaces, or all interfaces (Global Config mode). If an interface which has GARP enabled is enabled for routing or is enlisted as a member of a port-channel (LAG), GARP functionality is disabled on that interface. GARP functionality is subsequently re-enabled if routing is disabled and port-channel (LAG) membership is removed from an interface that has GARP enabled.

Default	disabled
Format	`set gmrp interfacemode`
Mode	◆ Interface Config ◆ Global Config

no set gmrp interfacemode

This command disables GARP Multicast Registration Protocol on a single interface or all interfaces. If an interface which has GARP enabled is enabled for routing or is enlisted as a member of a port-channel (LAG), GARP functionality is disabled. GARP functionality is subsequently re-enabled if routing is disabled and port-channel (LAG) membership is removed from an interface that has GARP enabled.

Format	`no set gmrp interfacemode`
Mode	◆ Interface Config ◆ Global Config

show gmrp configuration

This command displays Generic Attributes Registration Protocol (GARP) information for one or all interfaces.

Format	`show gmrp configuration {slot/port | all}`
Mode	◆ Privileged EXEC ◆ User EXEC

Term	Definition
Interface	The slot/port of the interface that this row in the table describes.

Term	Definition
Join Timer	The interval between the transmission of GARP PDUs registering (or reregistering) membership for an attribute. Current attributes are a VLAN or multicast group. There is an instance of this timer on a per-port, per-GARP participant basis. Permissible values are 10 to 100 centiseconds (0.1 to 1.0 seconds). The factory default is 20 centiseconds (0.2 seconds). The finest granularity of specification is 1 centisecond (0.01 seconds).
Leave Timer	The period of time to wait after receiving an unregister request for an attribute before deleting the attribute. Current attributes are a VLAN or multicast group. This may be considered a buffer time for another station to assert registration for the same attribute in order to maintain uninterrupted service. There is an instance of this timer on a per-Port, per-GARP participant basis. Permissible values are 20 to 600 centiseconds (0.2 to 6.0 seconds). The factory default is 60 centiseconds (0.6 seconds).
LeaveAll Timer	This Leave All Time controls how frequently LeaveAll PDUs are generated. A LeaveAll PDU indicates that all registrations will shortly be deregistered. Participants will need to rejoin in order to maintain registration. There is an instance of this timer on a per-Port, per-GARP participant basis. The Leave All Period Timer is set to a random value in the range of LeaveAllTime to 1.5*LeaveAllTime. Permissible values are 200 to 6000 centiseconds (2 to 60 seconds). The factory default is 1000 centiseconds (10 seconds).
Port GMRP Mode	The GMRP administrative mode for the port. It may be enabled or disabled. If this parameter is disabled, Join Time, Leave Time and Leave All Time have no effect.

show mac-address-table gmrp

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

Format	`show mac-address-table gmrp`
Mode	Privileged EXEC

Term	Definition
VLAN ID	The VLAN in which the MAC Address is learned.
MAC Address	A unicast MAC address for which the switch has forwarding and or filtering information. The format is 6 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB.
Type	The type of the entry. Static entries are those that are configured by the end user. Dynamic entries are added to the table as a result of a learning process or protocol.
Description	The text description of this multicast table entry.
Interfaces	The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).

Port-Based Network Access Control Commands

This section describes the commands you use to configure port-based network access control (IEEE 802.1X). Port-based network access control allows you to permit access to network services only to and devices that are authorized and authenticated.

aaa authentication dot1x default

Use this command to configure the authentication method for port-based access to the switch. The additional methods of authentication are used only if the previous method returns an error, not if there is an authentication failure. The possible methods are as follows:

- ias. Uses the internal authentication server users database for authentication. This method can be used in conjunction with any one of the existing methods like **local**, **radius**, etc.
- local. Uses the local username database for authentication.
- none. Uses no authentication.
- radius. Uses the list of all RADIUS servers for authentication.

Format	`aaa authentication dot1x default {[ias]|[`*`method1 [method2 [method3]]]`*`}`
Mode	Global Config

The following is an example of the command.

```
Broadcom FASTPATH Routing) #
(CN1610) #configure
(CN1610) (Config)#aaa authentication dot1x default ias none
(CN1610) (Config)#aaa authentication dot1x default ias local radius
none
```

clear dot1x statistics

This command resets the 802.1X statistics for the specified port or for all ports.

Format	`clear dot1x statistics {slot/port | all}`
Mode	Privileged EXEC

clear dot1x authentication-history

This command clears the authentication history table captured during successful and unsuccessful authentication on all interface or the specified interface.

Format	`clear dot1x authentication-history [slot/port]`
Mode	Privileged EXEC

clear radius statistics

This command is used to clear all RADIUS statistics.

Format	`clear radius statistics`
Mode	Privileged EXEC

dot1x eapolflood

Use this command to enable EAPOL flood support on the switch.

Default	disabled
Format	`dot1x eapolflood`
Mode	Global Config

no dot1x eapolflood

This command disables EAPOL flooding on the switch.

Format	`no dot1x eapolflood`
Mode	Global Config

dot1x dynamic-vlan enable

Use this command to enable the switch to create VLANs dynamically when a RADIUS-assigned VLAN does not exist in the switch.

Default	Disabled
Format	`dot1x dynamic-vlan enable`
Mode	Global Config

no dot1x dynamic-vlan enable

Use this command to prevent the switch from creating VLANs when a RADIUS-assigned VLAN does not exist in the switch.

Format	`no dot1x dynamic-vlan enable`
Mode	Global Config

dot1x guest-vlan

This command configures VLAN as guest vlan on an interface or a range of interfaces. The command specifies an active VLAN as an IEEE 802.1X guest VLAN. The range is 1 to the maximum VLAN ID supported by the platform.

Default	disabled
Format	`dot1x guest-vlan` *`vlan-id`*
Mode	Interface Config

no dot1x guest-vlan

This command disables Guest VLAN on the interface.

Default	disabled
Format	`no dot1x guest-vlan`
Mode	Interface Config

dot1x initialize

This command begins the initialization sequence on the specified port. This command is only valid if the control mode for the specified port is auto or mac-based. If the control mode is not auto or mac-based, an error will be returned.

Format	`dot1x initialize slot/port`
Mode	Privileged EXEC

dot1x max-req

This command sets the maximum number of times the authenticator state machine on an interface or range of interfaces will transmit an EAPOL EAP Request/Identity frame before timing out the supplicant. The *count* value must be in the range 1 - 10.

Default	2
Format	`dot1x max-req` *count*
Mode	Interface Config

no dot1x max-req

This command sets the maximum number of times the authenticator state machine on this port will transmit an EAPOL EAP Request/Identity frame before timing out the supplicant.

Format	`no dot1x max-req`
Mode	Interface Config

dot1x max-users

Use this command to set the maximum number of clients supported on an interface or range of interfaces when MAC-based dot1x authentication is enabled on the port. The maximum users supported per port is dependent on the product. The *count* value is in the range 1 - 48.

Default	48
Format	`dot1x max-users` *count*
Mode	Interface Config

no dot1x max-users

This command resets the maximum number of clients allowed per port to its default value.

Format	`no dot1x max-users`
Mode	Interface Config

dot1x port-control

This command sets the authentication mode to use on the specified interface or range of interfaces. Use the `force-unauthorized` parameter to specify that the authenticator PAE unconditionally sets the controlled port to unauthorized. Use the `force-authorized` parameter to specify that the authenticator PAE unconditionally sets the controlled port to authorized. Use the `auto` parameter to specify that the authenticator PAE sets the controlled port mode to reflect the outcome of the authentication exchanges between the supplicant, authenticator and the authentication server. If the `mac-based` option is specified, then MAC-based dot1x authentication is enabled on the port.

Default	auto
Format	`dot1x port-control {force-unauthorized | force-authorized | auto | mac-based}`
Mode	Interface Config

no dot1x port-control

This command sets the 802.1X port control mode on the specified port to the default value.

Format	`no dot1x port-control`
Mode	Interface Config

dot1x port-control all

This command sets the authentication mode to use on all ports. Select `force-unauthorized` to specify that the authenticator PAE unconditionally sets the controlled port to unauthorized. Select `force-authorized` to specify that the authenticator PAE unconditionally sets the controlled port to authorized. Select `auto` to specify that the authenticator PAE sets the controlled port mode to reflect the outcome of the authentication exchanges between the supplicant, authenticator and the authentication server. If the `mac-based` option is specified, then MAC-based dot1x authentication is enabled on the port.

Default	auto
Format	`dot1x port-control all {force-unauthorized | force-authorized | auto | mac-based}`
Mode	Global Config

no dot1x port-control all

This command sets the authentication mode on all ports to the default value.

Format	`no dot1x port-control all`
Mode	Global Config

dot1x mac-auth-bypass

If the 802.1X mode on the interface is mac-based, you can optionally use this command to enable MAC Authentication Bypass (MAB) on an interface. MAB is a supplemental authentication mechanism that allows 802.1X unaware clients – such as printers, fax machines, and some IP phones — to authenticate to the network using the client MAC address as an identifier.

Default	disabled
Format	`dot1x mac-auth-bypass`
Mode	Interface Config

no dot1x mac-auth-bypass

This command sets the MAB mode on the ports to the default value.

Format	`no dot1x mac-auth-bypass`
Mode	Interface Config

dot1x re-authenticate

This command begins the reauthentication sequence on the specified port. This command is only valid if the control mode for the specified port is **auto** or **mac-based**. If the control mode is not **auto** or **mac-based**, an error will be returned.

Format	`dot1x re-authenticate slot/port`
Mode	Privileged EXEC

dot1x re-authentication

This command enables reauthentication of the supplicant for the specified interface or range of interfaces.

Default	disabled

Format	`dot1x re-authentication`
Mode	Interface Config

no dot1x re-authentication

This command disables reauthentication of the supplicant for the specified port.

Format	`no dot1x re-authentication`
Mode	Interface Config

dot1x system-auth-control

Use this command to enable the dot1x authentication support on the switch. While disabled, the dot1x configuration is retained and can be changed, but is not activated.

Default	disabled
Format	`dot1x system-auth-control`
Mode	Global Config

no dot1x system-auth-control

This command is used to disable the dot1x authentication support on the switch.

Format	`no dot1x system-auth-control`
Mode	Global Config

dot1x system-auth-control monitor

Use this command to enable the 802.1X monitor mode on the switch. The purpose of Monitor mode is to help troubleshoot port-based authentication configuration issues without disrupting network access for hosts connected to the switch. In Monitor mode, a host is granted network access to an 802.1X-enabled port even if it fails the authentication process. The results of the process are logged for diagnostic purposes.

Default	disabled
Format	`dot1x system-auth-control monitor`

Mode	Global Config

no dot1x system-auth-control monitor

This command disables the 802.1X Monitor mode on the switch.

Format	`no dot1x system-auth-control monitor`
Mode	Global Config

dot1x timeout

This command sets the value, in seconds, of the timer used by the authenticator state machine on an interface or range of interfaces. Depending on the token used and the value (in seconds) passed, various timeout configurable parameters are set. The following tokens are supported:

Tokens	Definition
guest-vlan-period	The time, in seconds, for which the authenticator waits to see if any EAPOL packets are received on a port before authorizing the port and placing the port in the guest vlan (if configured). The guest vlan timer is only relevant when guest vlan has been configured on that specific port.
reauth-period	The value, in seconds, of the timer used by the authenticator state machine on this port to determine when reauthentication of the supplicant takes place. The reauth-period must be a value in the range 1 - 65535.
quiet-period	The value, in seconds, of the timer used by the authenticator state machine on this port to define periods of time in which it will not attempt to acquire a supplicant. The quiet-period must be a value in the range 0 - 65535.

Tokens	Definition
tx-period	The value, in seconds, of the timer used by the authenticator state machine on this port to determine when to send an EAPOL EAP Request/Identity frame to the supplicant. The quiet-period must be a value in the range 1 - 65535.
supp-timeout	The value, in seconds, of the timer used by the authenticator state machine on this port to timeout the supplicant. The supp-timeout must be a value in the range 1 - 65535.
server-timeout	The value, in seconds, of the timer used by the authenticator state machine on this port to timeout the authentication server. The supp-timeout must be a value in the range 1 - 65535.

Default	◆ guest-vlan-period: 90 seconds ◆ reauth-period: 3600 seconds ◆ quiet-period: 60 seconds ◆ tx-period: 30 seconds ◆ supp-timeout: 30 seconds ◆ server-timeout: 30 seconds
Format	`dot1x timeout {{guest-vlan-period` *`seconds`*`} |{reauth-period` *`seconds`*`} | {quiet-period` *`seconds`*`} | {tx-period` *`seconds`*`} | {supp-timeout` *`seconds`*`} | {server-timeout` *`seconds`*`}}`
Mode	Interface Config

no dot1x timeout

This command sets the value, in seconds, of the timer used by the authenticator state machine on this port to the default values. Depending on the token used, the corresponding default values are set.

Format	`no dot1x timeout {guest-vlan-period | reauth-period | quiet-period | tx-period | supp-timeout | server-timeout}`

Mode	Interface Config

dot1x unauthenticated-vlan

Use this command to configure the unauthenticated VLAN associated with the specified interface or range of interfaces. The unauthenticated VLAN ID can be a valid VLAN ID from 0-Maximum supported VLAN ID (4093 for FASTPATH). The unauthenticated VLAN must be statically configured in the VLAN database to be operational. By default, the unauthenticated VLAN is 0, i.e. invalid and not operational.

Default	0
Format	`dot1x unauthenticated-vlan` *`vlan id`*
Mode	Interface Config

no dot1x unauthenticated-vlan

This command resets the unauthenticated-vlan associated with the port to its default value.

Format	`no dot1x unauthenticated-vlan`
Mode	Interface Config

dot1x user

This command adds the specified user to the list of users with access to the specified port or all ports. The *`user`* parameter must be a configured user.

Format	`dot1x user` *`user`* `{slot/port | all}`
Mode	Global Config

no dot1x user

This command removes the user from the list of users with access to the specified port or all ports.

Format	`no dot1x user` *`user`* `{slot/port | all}`
Mode	Global Config

authentication enable

This command globally enables the Authentication Manager. Interface configuration takes effect only if the Authentication Manager is enabled with this command.

Default	disabled
Format	*authentication enable*
Mode	Global Config

no authentication enable

This command disables the Authentication Manager.

Format	*no authentication enable*
Mode	Global Config

authentication order

This command sets the order of authentication methods used on a port. The available authentication methods are Dot1x, MAB, and captive portal. Ordering sets the order of methods that the switch attempts when trying to authenticate a new device connected to a port. If one method is unsuccessful or timed out, the next method is attempted.

Each method can only be entered once. Ordering is only possible between 802.1x and MAB. Captive portal can be configured either as a stand-alone method or as the last method in the order.

Format	`authentication order {dot1x [mab [captive-portal] | captive-portal] | mab [dot1x [captive-portal]| captive-portal] | captive-portal}`
Mode	Interface Config

no authentication order

This command returns the port to the default authentication order.

Format	*no authentication order*
Mode	Interface Config

authentication priority

This command sets the priority for the authentication methods used on a port. The available authentication methods are Dot1x, MAB, and captive portal. The authentication priority decides if a previously authenticated client is reauthenticated with a higher-priority method when the same is received. Captive portal is always the last method in the list.

Default	`authentication order dot1x mab captive portal`
Format	`authentication priority {dot1x [mab [captive portal] | captive portal] | mab [dot1x [captive portal]| captive portal] | captive portal}`
Mode	Interface Config

no authentication priority

This command returns the port to the default order of priority for the authentication methods.

Format	*`no authentication priority`*
Mode	Interface Config

authentication restart

This command sets the time, in seconds, after which reauthentication starts. (The default time is 300 seconds.) The timer restarts the authentication only after all the authentication methods fail. At the expiration of this timer, authentication is reinitiated for the port.

Format	*`authentication restart <300-65535>`*
Mode	Interface Config

no authentication restart

This command sets the reauthentication value to the default value of 3600 seconds.

Format	*`no authentication restart`*
Mode	Interface Config

show authentication authentication-history

Use this command to display information about the authentication history for a specified interface.

Format	`show authentication authentication-history slot/port`
Mode	Privileged EXEC

Term	Definition
Time Stamp	The time of the authentication.
Interface	The interface.
MAC-Address	The MAC address for the interface.
Auth Status Method	The authentication method and status for the interface.

The following information is shown for the interface.

```
Time Stamp            Interface MAC-Address     Auth Status  Method
--------------------- --------- ----------------- ------ ----------
--
Jul 21 1919 15:06:15  1/0/1     00:00:00:00:00:01 Authorized  802.1X
```

show authentication interface

Use this command to display authentication method information either for all interfaces or a specified port.

Format	`show authentication interface {all | slot/port}`
Mode	Privileged EXEC

The following information is displayed for each interface.

Term	Definition
Interface	The interface for which authentication configuration information is being displayed.
Authentication Restart timer	The time, in seconds, after which reauthentication starts.

Term	Definition
Configured method order	The order of authentication methods used on a port.
Enabled method order	The order of authentication methods used on a port.
Configured method priority	The priority for the authentication methods used on a port.
Enabled method priority	The priority for the authentication methods used on a port.
Number of authenticated clients	The number of authenticated clients.
Logical Interface	The logical interface
Client MAC addr	The MAC address for the client.
Authenticated Method	The current authentication method.
Auth State	If the authentication was successful.
Auth Status	The current authentication status.

The following example displays the authentication interface information for all interfaces.

```
(CN1610) #show authentication interface all

Interface..................................... 1/0/1
Authentication Restart timer.................. 300
Configured method order....................... dot1x mab captive-
portal
Enabled method order.......................... dot1x mab undefined
Configured method priority..................... undefined undefined
undefined
Enabled method priority....................... undefined undefined
undefined
Number of authenticated clients............... 0
Interface..................................... 1/0/2
Authentication Restart timer.................. 300
Configured method order....................... dot1x mab captive-
portal
Enabled method order.......................... dot1x mab undefined
```

```
Configured method priority..... undefined undefined
undefined
Enabled method priority..... undefined undefined
undefined
Number of authenticated clients..... 0
Interface..... 1/0/3
Authentication Restart timer..... 300
Configured method order..... dot1x mab captive-
portal
Enabled method order..... dot1x mab undefined
Configured method priority..... undefined undefined
undefined
Enabled method priority..... undefined undefined
undefined
Number of authenticated clients..... 0
Interface..... 1/0/4
Authentication Restart timer..... 300
Configured method order..... dot1x mab captive-
portal
Enabled method order..... dot1x mab undefined
Configured method priority..... undefined undefined
undefined
Enabled method priority..... undefined undefined
undefined
Number of authenticated clients..... 0
```

show authentication methods

Use this command to display information about the authentication methods.

Format	`show authentication methods`
Mode	Privileged EXEC

Term	Definition
Authentication Login List	The authentication login listname.
Method 1	The first method in the specified authentication login list, if any.
Method 2	The second method in the specified authentication login list, if any.

Term	Definition
Method 3	The third method in the specified authentication login list, if any.

The following example displays the authentication configuration.

```
(CN1610) #show authentication methods

Login Authentication Method Lists
---------------------------------
defaultList         :  local
networkList         :  local

Enable Authentication Method Lists
----------------------------------
enableList          :  enable   none
enableNetList       :  enable   deny

Line     Login Method List    Enable Method List
-------  -----------------    ------------------
Console  defaultList          enableList
Telnet   networkList          enableList
SSH      networkList          enableList

DOT1X       :
```

show authentication statistics

Use this command to display the authentication statistics for an interface.

Format	`show authentication statistics slot/port`
Mode	Privileged EXEC

The following information is displayed for each interface.

Term	Definition
Port	The port for which information is being displayed.
802.1X attempts	The number of Dot1x authentication attempts for the port.

Term	Definition
802.1X failed attempts	The number of failed Dot1x authentication attempts for the port.
Mab attempts	The number of MAB (MAC authentication bypass) authentication attempts for the port.
Mab failed attempts	The number of failed MAB authentication attempts for the port.
Captive-portal attempts	The number of captive portal authentication attempts for the port.
Captive-portal failed attempts	The number of failed captive portal authentication attempts for the port.

```
(CN1610) #show authentication statistics 1/0/1

Port..................................... 1/0/1
802.1X attempts.......................... 0
802.1X failed attempts................... 0
Mab attempts............................. 0
Mab failed attempts...................... 0
Captive-portal attempts.................. 0
Captive-Portal failed attempts........... 0
```

clear authentication statistics

Use this command to clear the authentication statistics on an interface.

Format	`clear authentication authentication-history {slot/port] | all}`
Mode	Privileged EXEC

clear authentication authentication-history

Use this command to clear the authentication history log for an interface.

Format	`clear authentication authentication-history {slot/port | all}`
Mode	Privileged EXEC

show dot1x

This command is used to show a summary of the global dot1x configuration, summary information of the dot1x configuration for a specified port or all ports, the detailed dot1x configuration for a specified port and the dot1x statistics for a specified port - depending on the tokens used.

Format	`show dot1x [{summary {slot/port | all} | detail slot/port | statistics slot/port]`
Mode	Privileged EXEC

If you do not use the optional parameters *unit/slot/port* or *vlanid*, the command displays the global dot1x mode, the VLAN Assignment mode, and the Dynamic VLAN Creation mode.

Term	Definition
Administrative Mode	Indicates whether authentication control on the switch is enabled or disabled.
VLAN Assignment Mode	Indicates whether assignment of an authorized port to a RADIUS-assigned VLAN is allowed (enabled) or not (disabled).
Dynamic VLAN Creation Mode	Indicates whether the switch can dynamically create a RADIUS-assigned VLAN if it does not currently exist on the switch.
Monitor Mode	Indicates whether the Dot1x Monitor mode on the switch is enabled or disabled.

If you use the optional parameter *summary* {slot/port | all}, the dot1x configuration for the specified port or all ports are displayed.

Term	Definition
Interface	The interface whose configuration is displayed.
Control Mode	The configured control mode for this port. Possible values are force-unauthorized | force-authorized | auto | mac-based | authorized | unauthorized.

Term	Definition
Operating Control Mode	The control mode under which this port is operating. Possible values are authorized | unauthorized.
Reauthentication Enabled	Indicates whether reauthentication is enabled on this port.
Port Status	Indicates whether the port is authorized or unauthorized. Possible values are authorized | unauthorized.

The following shows example CLI display output for the command `show dot1x summary 0/1.`

```
Operating
Interface Control Mode Control Mode Port Status
--------- ----------------------- ------------
0/1 auto auto Authorized
```

If you use the optional parameter '`detail` slot/port', the detailed dot1x configuration for the specified port is displayed.

Term	Definition
Port	The interface whose configuration is displayed.
Protocol Version	The protocol version associated with this port. The only possible value is 1, corresponding to the first version of the dot1x specification.
PAE Capabilities	The port access entity (PAE) functionality of this port. Possible values are Authenticator or Supplicant.
Control Mode	The configured control mode for this port. Possible values are force-unauthorized | force-authorized | auto | mac-based.

Term	Definition
Authenticator PAE State	Current state of the authenticator PAE state machine. Possible values are Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, ForceAuthorized, and ForceUnauthorized. When MAC-based authentication is enabled on the port, this parameter is deprecated.
Backend Authentication State	Current state of the backend authentication state machine. Possible values are Request, Response, Success, Fail, Timeout, Idle, and Initialize. When MAC-based authentication is enabled on the port, this parameter is deprecated.
Quiet Period	The timer used by the authenticator state machine on this port to define periods of time in which it will not attempt to acquire a supplicant. The value is expressed in seconds and will be in the range 0 and 65535.
Transmit Period	The timer used by the authenticator state machine on the specified port to determine when to send an EAPOL EAP Request/Identity frame to the supplicant. The value is expressed in seconds and will be in the range of 1 and 65535.
Guest-VLAN ID	The guest VLAN identifier configured on the interface.
Guest VLAN Period	The time in seconds for which the authenticator waits before authorizing and placing the port in the Guest VLAN, if no EAPOL packets are detected on that port.

Term	Definition
Supplicant Timeout	The timer used by the authenticator state machine on this port to timeout the supplicant. The value is expressed in seconds and will be in the range of 1 and 65535.
Server Timeout	The timer used by the authenticator on this port to timeout the authentication server. The value is expressed in seconds and will be in the range of 1 and 65535.
Maximum Requests	The maximum number of times the authenticator state machine on this port will retransmit an EAPOL EAP Request/Identity before timing out the supplicant. The value will be in the range of 1 and 10.
Configured MAB Mode	The administrative mode of the MAC authentication bypass feature on the switch.
Operational MAB Mode	The operational mode of the MAC authentication bypass feature on the switch. MAB might be administratively enabled but not operational if the control mode is not MAC based.
Vlan-ID	The VLAN assigned to the port by the radius server. This is only valid when the port control mode is not Mac-based.
VLAN Assigned Reason	The reason the VLAN identified in the VLAN-assigned field has been assigned to the port. Possible values are RADIUS, Unauthenticated VLAN, Guest VLAN, default, and Not Assigned. When the VLAN Assigned Reason is Not Assigned, it means that the port has not been assigned to any VLAN by dot1x. This only valid when the port control mode is not MAC-based.
Reauthentication Period	The timer used by the authenticator state machine on this port to determine when reauthentication of the supplicant takes place. The value is expressed in seconds and will be in the range of 1 and 65535.

Term	Definition
Reauthentication Enabled	Indicates if reauthentication is enabled on this port. Possible values are ‘True” or “False”.
Key Transmission Enabled	Indicates if the key is transmitted to the supplicant for the specified port. Possible values are True or False.
EAPOL Flood Mode Enabled	Indicates whether the EAPOL flood support is enabled on the switch. Possible values are True or False.
Control Direction	The control direction for the specified port or ports. Possible values are both or in.
Maximum Users	The maximum number of clients that can get authenticated on the port in the MAC-based dot1x authentication mode. This value is used only when the port control mode is not MAC-based.
Unauthenticated VLAN ID	Indicates the unauthenticated VLAN configured for this port. This value is valid for the port only when the port control mode is not MAC-based.
Session Timeout	Indicates the time for which the given session is valid. The time period in seconds is returned by the RADIUS server on authentication of the port. This value is valid for the port only when the port control mode is not MAC-based.
Session Termination Action	This value indicates the action to be taken once the session timeout expires. Possible values are Default, Radius-Request. If the value is Default, the session is terminated the port goes into unauthorized state. If the value is Radius-Request, then a reauthentication of the client authenticated on the port is performed. This value is valid for the port only when the port control mode is not MAC-based.

The following shows example CLI display output for the command.

```
(CN1610) #show dot1x detail 1/0/3
```

```
Port..................................... 1/0/1
Protocol Version......................... 1
PAE Capabilities......................... Authenticator
Control Mode............................. auto
Authenticator PAE State.................. Initialize
Backend Authentication State............. Initialize
Quiet Period (secs)...................... 60
Transmit Period (secs)................... 30
Guest VLAN ID............................ 0
Guest VLAN Period (secs)................. 90
Supplicant Timeout (secs)................ 30
Server Timeout (secs).................... 30
Maximum Requests......................... 2
Configured MAB Mode...................... Enabled
Operational MAB Mode..................... Disabled
VLAN Id.................................. 0
VLAN Assigned Reason..................... Not Assigned
Reauthentication Period (secs)........... 3600
Reauthentication Enabled................. FALSE
Key Transmission Enabled................. FALSE
EAPOL flood Mode Enabled................. FALSE
Control Direction........................ both
Maximum Users............................ 16
Unauthenticated VLAN ID.................. 0
Session Timeout.......................... 0
Session Termination Action............... Default
```

For each client authenticated on the port, the `show dot1x detail` slot/port command will display the following MAC-based dot1x parameters if the port-control mode for that specific port is MAC-based.

Term	Definition
Supplicant MAC-Address	The MAC-address of the supplicant.
Authenticator PAE State	Current state of the authenticator PAE state machine. Possible values are Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, ForceAuthorized, and ForceUnauthorized.
Backend Authentication State	Current state of the backend authentication state machine. Possible values are Request, Response, Success, Fail, Timeout, Idle, and Initialize.

Term	Definition
VLAN-Assigned	The VLAN assigned to the client by the radius server.
Logical Port	The logical port number associated with the client.

If you use the optional parameter `statistics` slot/port, the following dot1x statistics for the specified port appear.

Term	Definition
Port	The interface whose statistics are displayed.
EAPOL Frames Received	The number of valid EAPOL frames of any type that have been received by this authenticator.
EAPOL Frames Transmitted	The number of EAPOL frames of any type that have been transmitted by this authenticator.
EAPOL Start Frames Received	The number of EAPOL start frames that have been received by this authenticator.
EAPOL Logoff Frames Received	The number of EAPOL logoff frames that have been received by this authenticator.
Last EAPOL Frame Version	The protocol version number carried in the most recently received EAPOL frame.
Last EAPOL Frame Source	The source MAC address carried in the most recently received EAPOL frame.
EAP Response/Id Frames Received	The number of EAP response/identity frames that have been received by this authenticator.
EAP Response Frames Received	The number of valid EAP response frames (other than resp/id frames) that have been received by this authenticator.
EAP Request/Id Frames Transmitted	The number of EAP request/identity frames that have been transmitted by this authenticator.

Term	Definition
EAP Request Frames Transmitted	The number of EAP request frames (other than request/identity frames) that have been transmitted by this authenticator.
Invalid EAPOL Frames Received	The number of EAPOL frames that have been received by this authenticator in which the frame type is not recognized.
EAP Length Error Frames Received	The number of EAPOL frames that have been received by this authenticator in which the frame type is not recognized.

show dot1x authentication-history

This command displays 802.1X authentication events and information during successful and unsuccessful Dot1x authentication process for all interfaces or the specified interface. Use the optional keywords to display only failure authentication events in summary or in detail.

Format	`show dot1x authentication-history {slot/port | all} [failed-auth-only] [detail]`
Mode	Privileged EXEC

Term	Definition
Time Stamp	The exact time at which the event occurs.
Interface	Physical Port on which the event occurs.
Mac-Address	The supplicant/client MAC address.
VLAN assigned	The VLAN assigned to the client/port on authentication.
VLAN assigned Reason	The type of VLAN ID assigned, which can be Guest VLAN, Unauth, Default, RADIUS Assign or Montior Mode VLAN ID.
Auth Status	The authentication status.
Reason	The actual reason behind the successful or failed authentication.

show dot1x clients

This command displays 802.1X client information. This command also displays information about the number of clients that are authenticated using Monitor mode and using 802.1X.

Format	`show dot1x clients {slot/port | all}`
Mode	Privileged EXEC

Term	Definition
Clients Authenticated using Monitor Mode	Indicates the number of the Dot1x clients authenticated using Monitor mode.
Clients Authenticated using Dot1x	Indicates the number of Dot1x clients authenticated using 802.1x authentication process.
Logical Interface	The logical port number associated with a client.
Interface	The physical port to which the supplicant is associated.
User Name	The user name used by the client to authenticate to the server.
Supplicant MAC Address	The supplicant device MAC address.
Session Time	The time since the supplicant is logged on.
Filter ID	Identifies the Filter ID returned by the RADIUS server when the client was authenticated. This is a configured DiffServ policy name on the switch.
VLAN ID	The VLAN assigned to the port.
VLAN Assigned	The reason the VLAN identified in the VLAN ID field has been assigned to the port. Possible values are RADIUS, Unauthenticated VLAN, Monitor Mode, or Default. When the VLAN Assigned reason is Default, it means that the VLAN was assigned to the port because the P-VID of the port was that VLAN ID.

Term	Definition
Session Timeout	This value indicates the time for which the given session is valid. The time period in seconds is returned by the RADIUS server on authentication of the port. This value is valid for the port only when the port-control mode is not MAC-based.
Session Termination Action	This value indicates the action to be taken once the session timeout expires. Possible values are Default and Radius-Request. If the value is Default, the session is terminated and client details are cleared. If the value is Radius-Request, then a reauthentication of the client is performed.

show dot1x users

This command displays 802.1X port security user information for locally configured users.

Format	`show dot1x users slot/port`
Mode	Privileged EXEC

Term	Definition
Users	Users configured locally to have access to the specified port.

802.1X Supplicant Commands

FASTPATH supports 802.1X (“dot1x”) supplicant functionality on point-to-point ports. The administrator can configure the user name and password used in authentication and capabilities of the supplicant port.

dot1x pae

This command sets the port’s dot1x role. The port can serve as either a supplicant or an authenticator.

Format	`dot1x pae {supplicant | authenticator}`
Mode	Interface Config

dot1x supplicant port-control

This command sets the ports authorization state (Authorized or Unauthorized) either manually or by setting the port to auto-authorize upon startup. By default all the ports are authenticators. If the port’s attribute needs to be moved from <authenticator to supplicant> or <supplicant to authenticator>, use this command.

Format	`dot1x supplicant port-control {auto | force-authorized | force_unauthorized}`
Mode	Interface Config

Parameter	Description
auto	The port is in the Unauthorized state until it presents its user name and password credentials to an authenticator. If the authenticator authorizes the port, then it is placed in the Authorized state.
force-authorized	Sets the authorization state of the port to Authorized, bypassing the authentication process.
force-unauthorized	Sets the authorization state of the port to Unauthorized, bypassing the authentication process.

no dot1x supplicant port-control

This command sets the port-control mode to the default, auto.

Default	auto
Format	`no dot1x supplicant port-control`
Mode	Interface Config

dot1x supplicant max-start

This command configures the number of attempts that the supplicant makes to find the authenticator before the supplicant assumes that there is no authenticator.

Default	3
Format	`dot1x supplicant max-start` *<1-10>*
Mode	Interface Config

no dot1x supplicant max-start

This command sets the max-start value to the default.

Format	`no dot1x supplicant max-start`
Mode	Interface Config

dot1x supplicant timeout start-period

This command configures the start period timer interval to wait for the EAP identity request from the authenticator.

Default	30 seconds
Format	`dot1x supplicant timeout start-period` *<1-65535 seconds>*
Mode	Interface Config

no dot1x supplicant timeout start-period

This command sets the start-period value to the default.

Format	`no dot1x supplicant timeout start-period`
Mode	Interface Config

dot1x supplicant timeout held-period

This command configures the held period timer interval to wait for the next authentication on previous authentication fail.

Default	60 seconds
Format	`dot1x supplicant timeout held-period <1-65535 seconds>`
Mode	Interface Config

no dot1x supplicant timeout held-period

This command sets the held-period value to the default value.

Format	`no dot1x supplicant timeout held-period`
Mode	Interface Config

dot1x supplicant timeout auth-period

This command configures the authentication period timer interval to wait for the next EAP request challenge from the authenticator.

Default	30 seconds
Format	`dot1x supplicant timeout auth-period <1-65535 seconds>`
Mode	Interface Config

no dot1x supplicant timeout auth-period

This command sets the auth-period value to the default value.

Format	`no dot1x supplicant timeout auth-period`
Mode	Interface Config

dot1x supplicant user

Use this command to map the given user to the port.

Format	`dot1x supplicant user`
Mode	Interface Config

show dot1x statistics

This command displays the dot1x port statistics in detail.

Format	`show dot1x statistics` *slot/port*
Mode	◆ Privileged EXEC ◆ User EXEC

Term	Definition
EAPOL Frames Received	Displays the number of valid EAPOL frames received on the port.
EAPOL Frames Transmitted	Displays the number of EAPOL frames transmitted via the port.
EAPOL Start Frames Transmitted	Displays the number of EAPOL Start frames transmitted via the port.
EAPOL Logoff Frames Received	Displays the number of EAPOL Log off frames that have been received on the port.
EAP Resp/ID Frames Received	Displays the number of EAP Respond ID frames that have been received on the port.
EAP Response Frames Received	Displays the number of valid EAP Respond frames received on the port.
EAP Req/ID Frames Transmitted	Displays the number of EAP Requested ID frames transmitted via the port.
EAP Req Frames Transmitted	Displays the number of EAP Request frames transmitted via the port.
Invalid EAPOL Frames Received	Displays the number of unrecognized EAPOL frames received on this port.
EAP Length Error Frames Received	Displays the number of EAPOL frames with an invalid Packet Body Length received on this port.
Last EAPOL Frames Version	Displays the protocol version number attached to the most recently received EAPOL frame.
Last EAPOL Frames Source	Displays the source MAC Address attached to the most recently received EAPOL frame.

The following shows example CLI display output for the command.

```
(CN1610) #show dot1x statistics 0/1
Port..................................... 0/1
EAPOL Frames Received.................... 0
EAPOL Frames Transmitted................. 0
EAPOL Start Frames Transmitted........... 3
EAPOL Logoff Frames Received............. 0
EAP Resp/Id frames transmitted........... 0
EAP Response frames transmitted.......... 0
EAP Req/Id frames transmitted............ 0
EAP Req frames transmitted............... 0
Invalid EAPOL frames received............ 0
EAP length error frames received......... 0
Last EAPOL Frame Version................. 0
Last EAPOL Frame Source.................. 00:00:00:00:02:01
```

Storm-Control Commands

This section describes commands you use to configure storm-control and view storm-control configuration information. A traffic storm is a condition that occurs when incoming packets flood the LAN, which creates performance degradation in the network. The Storm-Control feature protects against this condition.

FASTPATH provides broadcast, multicast, and unicast story recovery for individual interfaces. Unicast Storm-Control protects against traffic whose MAC addresses are not known by the system. For broadcast, multicast, and unicast storm-control, if the rate of traffic ingressing on an interface increases beyond the configured threshold for that type, the traffic is dropped.

To configure storm-control, you will enable the feature for all interfaces or for individual interfaces, and you will set the threshold (storm-control level) beyond which the broadcast, multicast, or unicast traffic will be dropped. The Storm-Control feature allows you to limit the rate of specific types of packets through the switch on a per-port, per-type, basis.

Configuring a storm-control level also enables that form of storm-control. Disabling a storm-control level (using the “no” version of the command) sets the storm-control level back to the default value and disables that form of storm-control. Using the “no” version of the “storm-control” command (not stating a “level”) disables that form of storm-control but maintains the configured “level” (to be active the next time that form of storm-control is enabled.)

Note

The actual rate of ingress traffic required to activate storm-control is based on the size of incoming packets and the hard-coded average packet size of 512 bytes - used to calculate a packet-per-second (pps) rate - as the forwarding-plane requires pps versus an absolute rate kbps. For example, if the configured limit is 10%, this is converted to ~25000 pps, and this pps limit is set in forwarding plane (hardware). You get the approximate desired output when 512bytes packets are used.

storm-control broadcast

Use this command to enable broadcast storm recovery mode for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode). If the mode is enabled, broadcast storm recovery is active and, if the rate of L2

broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of broadcast traffic will be limited to the configured threshold.

Default	disabled
Format	`storm-control broadcast`
Mode	◆ Global Config ◆ Interface Config

no storm-control broadcast

Use this command to disable broadcast storm recovery mode for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode).

Format	`no storm-control broadcast`
Mode	◆ Global Config ◆ Interface Config

storm-control broadcast level

Use this command to configure the broadcast storm recovery threshold for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) as a percentage of link speed and enable broadcast storm recovery. If the mode is enabled, broadcast storm recovery is active, and if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic is dropped. Therefore, the rate of broadcast traffic is limited to the configured threshold.

Default	5
Format	`storm-control broadcast level` *`0-100`*
Mode	◆ Global Config ◆ Interface Config

no storm-control broadcast level

This command sets the broadcast storm recovery threshold to the default value for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) and disables broadcast storm recovery.

Format	`no storm-control broadcast level`
Mode	◆ Global Config ◆ Interface Config

storm-control broadcast rate

Use this command to configure the broadcast storm recovery threshold for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) in packets per second. If the mode is enabled, broadcast storm recovery is active, and if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic is dropped. Therefore, the rate of broadcast traffic is limited to the configured threshold.

Default	0
Format	`storm-control broadcast rate` *`0-14880000`*
Mode	◆ Global Config ◆ Interface Config

no storm-control broadcast rate

This command sets the broadcast storm recovery threshold to the default value for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) and disables broadcast storm recovery.

Format	`no storm-control broadcast rate`
Mode	◆ Global Config ◆ Interface Config

storm-control multicast

This command enables multicast storm recovery mode for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode). If the mode is enabled, multicast storm recovery is active, and if the rate of L2 multicast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of multicast traffic will be limited to the configured threshold.

Default	disabled

Format	`storm-control multicast`
Mode	◆ Global Config ◆ Interface Config

no storm-control multicast

This command disables multicast storm recovery mode for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode).

Format	`no storm-control multicast`
Mode	◆ Global Config ◆ Interface Config

storm-control multicast level

This command configures the multicast storm recovery threshold for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) as a percentage of link speed and enables multicast storm recovery mode. If the mode is enabled, multicast storm recovery is active, and if the rate of L2 multicast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of multicast traffic will be limited to the configured threshold.

Default	5
Format	`storm-control multicast level` *`0-100`*
Mode	◆ Global Config ◆ Interface Config

no storm-control multicast level

This command sets the multicast storm recovery threshold to the default value for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) and disables multicast storm recovery.

Format	`no storm-control multicast level` *`0-100`*
Mode	◆ Global Config ◆ Interface Config

storm-control multicast rate

Use this command to configure the multicast storm recovery threshold for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) in packets per second. If the mode is enabled, multicast storm recovery is active, and if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic is dropped. Therefore, the rate of multicast traffic is limited to the configured threshold.

Default	0
Format	`storm-control multicast rate` *`0-14880000`*
Mode	◆ Global Config ◆ Interface Config

no storm-control multicast rate

This command sets the multicast storm recovery threshold to the default value for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) and disables multicast storm recovery.

Format	`no storm-control multicast rate`
Mode	◆ Global Config ◆ Interface Config

storm-control unicast

This command enables unicast storm recovery mode for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode). If the mode is enabled, unicast storm recovery is active, and if the rate of unknown L2 unicast (destination lookup failure) traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of unknown unicast traffic will be limited to the configured threshold.

Default	disabled
Format	`storm-control unicast`
Mode	◆ Global Config ◆ Interface Config

no storm-control unicast

This command disables unicast storm recovery mode for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode).

Format	`no storm-control unicast`
Mode	◆ Global Config ◆ Interface Config

storm-control unicast level

This command configures the unicast storm recovery threshold for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) as a percentage of link speed, and enables unicast storm recovery. If the mode is enabled, unicast storm recovery is active, and if the rate of unknown L2 unicast (destination lookup failure) traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of unknown unicast traffic will be limited to the configured threshold.This command also enables unicast storm recovery mode for an interface.

Default	5
Format	`storm-control unicast level` *`0-100`*
Mode	◆ Global Config ◆ Interface Config

no storm-control unicast level

This command sets the unicast storm recovery threshold to the default value for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) and disables unicast storm recovery.

Format	`no storm-control unicast level`
Mode	◆ Global Config ◆ Interface Config

storm-control unicast rate

Use this command to configure the unicast storm recovery threshold for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) in packets per second. If the mode is enabled, unicast storm recovery is

active, and if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic is dropped. Therefore, the rate of unicast traffic is limited to the configured threshold.

Default	0
Format	`storm-control unicast rate` *`0-14880000`*
Mode	◆ Global Config ◆ Interface Config

no storm-control unicast rate

This command sets the unicast storm recovery threshold to the default value for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) and disables unicast storm recovery.

Format	`no storm-control unicast rate`
Mode	◆ Global Config ◆ Interface Config

show storm-control

This command displays switch configuration information. If you do not use any of the optional parameters, this command displays global storm control configuration parameters:

- **Broadcast Storm Recovery Mode** may be enabled or disabled. The factory default is disabled.
- **802.3x Flow Control Mode** may be enabled or disabled. The factory default is disabled.

Use the `all` keyword to display the per-port configuration parameters for all interfaces, or specify the slot/port to display information about a specific interface.

Format	`show storm-control [all | slot/port]`
Mode	Privileged EXEC

Parameter	Definition
Bcast Mode	Shows whether the broadcast storm control mode is enabled or disabled. The factory default is disabled.
Bcast Level	The broadcast storm control level.
Mcast Mode	Shows whether the multicast storm control mode is enabled or disabled.
Mcast Level	The multicast storm control level.
Ucast Mode	Shows whether the Unknown Unicast or DLF (Destination Lookup Failure) storm control mode is enabled or disabled.
Ucast Level	The Unknown Unicast or DLF (Destination Lookup Failure) storm control level.

The following shows example CLI display output for the command.

```
(CN1610) #show storm-control
(CN1610) #show storm-control

Broadcast Storm Control Mode..................... Disable
Broadcast Storm Control Level.................... 5 percent
Multicast Storm Control Mode..................... Disable
Multicast Storm Control Level.................... 5 percent
Unicast Storm Control Mode....................... Disable
Unicast Storm Control Level...................... 5 percent
```

The following shows example CLI display output for the command.

```
(CN1610) #show storm-control 0/1

 Bcast   Bcast    Mcast   Mcast    Ucast   Ucast
 Intf   Mode    Level    Mode    Level    Mode    Level
------ ------- -------- ------- -------- ------- --------
0/1  Disable       5% Disable       5% Disable       5%
```

The following shows an example of part of the CLI display output for the command.

```
(CN1610) #show storm-control all

 Bcast   Bcast    Mcast   Mcast    Ucast   Ucast
```

```
 Intf   Mode    Level    Mode    Level    Mode    Level
------ ------- -------- ------- -------- ------- --------
0/1  Disable       5% Disable       5% Disable       5%
0/2  Disable       5% Disable       5% Disable       5%
0/3  Disable       5% Disable       5% Disable       5%
0/4  Disable       5% Disable       5% Disable       5%
0/5  Disable       5% Disable       5% Disable       5%
```

Link Local Protocol Filtering Commands

Link Local Protocol Filtering (LLPF) allows the switch to filter out multiple proprietary protocol PDUs, such as Port Aggregation Protocol (PAgP), if the problems occur with proprietary protocols running on standards-based switches. If certain protocol PDUs cause unexpected results, LLPF can be enabled to prevent those protocol PDUs from being processed by the switch.

llpf

Use this command to block LLPF protocol(s) on a port.

Default	Enabled for the blockudld parameter; disabled for all others.
Format	`llpf {blockisdp | blockvtp | blockdtp | blockudld | blockpagp | blocksstp | blockall}`
Mode	Interface Config

no llpf

Use this command to unblock LLPF protocol(s) on a port.

Format	`no llpf {blockisdp | blockvtp | blockdtp | blockudld | blockpagp | blocksstp | blockall }`
Mode	Interface Config

show llpf interface

Use this command to display the status of LLPF rules configured on a particular port or on all ports.

Format	`show llpf interface [all | slot/port]`
Mode	Privileged EXEC

Term	Definition
Block ISDP	Shows whether the port blocks ISDP PDUs.
Block VTP	Shows whether the port blocks VTP PDUs.

Term	Definition
Block DTP	Shows whether the port blocks DTP PDUs.
Block UDLD	Shows whether the port blocks UDLD PDUs.
Block PAGP	Shows whether the port blocks PAgP PDUs.
Block SSTP	Shows whether the port blocks SSTP PDUs.
Block All	Shows whether the port blocks all proprietary PDUs available for the LLDP feature.

Port-Channel/LAG (802.3ad) Commands

This section describes the commands you use to configure port-channels, which is defined in the 802.3ad specification, and that are also known as link aggregation groups (LAGs). Link aggregation allows you to combine multiple full-duplex Ethernet links into a single logical link. Network devices treat the aggregation as if it were a single link, which increases fault tolerance and provides load sharing. The LAG feature initially load shares traffic based upon the source and destination MAC address. Assign the port-channel (LAG) VLAN membership after you create a port-channel. If you do not assign VLAN membership, the port-channel might become a member of the management VLAN which can result in learning and switching issues.

A port-channel (LAG) interface can be either static or dynamic, but not both. All members of a port channel must participate in the same protocols.) A static port-channel interface does not require a partner system to be able to aggregate its member ports.

Note
If you configure the maximum number of supported dynamic port-channels (LAGs), additional port-channels that you configure are automatically static.

port-channel

This command configures a new port-channel (LAG) and generates a logical slot/port number for the port-channel. The *name* field is a character string which allows the dash "-" character as well as alphanumeric characters. Use the `show port channel` command to display the slot/port number for the logical interface. Instead of slot/port, `lag` *`lag-intf-num`* can be used as an alternate way to specify the LAG interface. `lag` *`lag-intf-num`* can also be used to specify the LAG interface where *`lag-intf-num`* is the LAG port number.

Note
Before you include a port in a port-channel, set the port physical mode. For more information, see "speed" on page 312.

Format	`port-channel` *`name`*
Mode	Global Config

addport

This command adds one port to the port-channel (LAG). The first interface is a logical slot/port number of a configured port-channel. You can add a range of ports by specifying the port range when you enter Interface Config mode (for example: `interface 0/1-0/4`. Instead of slot/port, `lag` *`lag-intf-num`* can be used as an alternate way to specify the LAG interface. `lag` *`lag-intf-num`* can also be used to specify the LAG interface where *`lag-intf-num`* is the LAG port number.

Note

Before adding a port to a port-channel, set the physical mode of the port. For more information, see "speed" on page 312.

Format	`addport` *`logical`* `slot/port`
Mode	Interface Config

deleteport (Interface Config)

This command deletes a port or a range of ports from the port-channel (LAG). The interface is a logical slot/port number of a configured port-channel (or range of port-channels). Instead of slot/port, `lag` *`lag-intf-num`* can be used as an alternate way to specify the LAG interface. `lag` *`lag-intf-num`* can also be used to specify the LAG interface where *`lag-intf-num`* is the LAG port number.

Format	`deleteport` *`logical`* `slot/port`
Mode	Interface Config

deleteport (Global Config)

This command deletes all configured ports from the port-channel (LAG). The interface is a logical slot/port number of a configured port-channel.Instead of slot/port, `lag` *`lag-intf-num`* can be used as an alternate way to specify the LAG interface. `lag` *`lag-intf-num`* can also be used to specify the LAG interface where *`lag-intf-num`* is the LAG port number.

Format	`deleteport {`*`logical`* `slot/port	all}`
Mode	Global Config

lacp admin key

Use this command to configure the administrative value of the key for the port-channel. The value range of *key* is 0 to 65535. This command can be used to configure a single interface or a range of interfaces.

Default	0x8000
Format	`lacp admin key` *key*
Mode	Interface Config

Note
This command is applicable only to port-channel interfaces.

no lacp admin key

Use this command to configure the default administrative value of the key for the port-channel.

Format	`no lacp admin key`
Mode	Interface Config

lacp collector max-delay

Use this command to configure the port-channel collector max delay. This command can be used to configure a single interface or a range of interfaces.The valid range of *delay* is 0-65535.

Default	0x8000
Format	`lacp collector max delay` *delay*
Mode	Interface Config

Note
This command is applicable only to port-channel interfaces.

no lacp collector max delay

Use this command to configure the default port-channel collector max delay.

Format	`no lacp collector max delay`
Mode	Interface Config

lacp actor admin key

Use this command to configure the administrative value of the LACP actor admin key on an interface or range of interfaces. The valid range for *key* is 0-65535.

Default	Internal Interface Number of this Physical Port
Format	`lacp actor admin key key`
Mode	Interface Config

Note
This command is applicable only to physical interfaces.

no lacp actor admin key

Use this command to configure the default administrative value of the key.

Format	`no lacp actor admin key`
Mode	Interface Config

lacp actor admin state individual

Use this command to set LACP actor admin state to individual.

Format	`lacp actor admin state individual`
Mode	Interface Config

Note
This command is applicable only to physical interfaces.

no lacp actor admin state individual

Use this command to set the LACP actor admin state to aggregation.

Format	`no lacp actor admin state individual`
Mode	Interface Config

lacp actor admin state longtimeout

Use this command to set LACP actor admin state to longtimeout.

Format	`lacp actor admin state longtimeout`

Mode	Interface Config

Note
This command is applicable only to physical interfaces.

no lacp actor admin state longtimeout

Use this command to set the LACP actor admin state to short timeout.

Format	`no lacp actor admin state longtimeout`
Mode	Interface Config

Note
This command is applicable only to physical interfaces.

lacp actor admin state passive

Use this command to set the LACP actor admin state to passive.

Format	`lacp actor admin state passive`
Mode	Interface Config

Note
This command is applicable only to physical interfaces.

no lacp actor admin state passive

Use this command to set the LACP actor admin state to active.

Format	`no lacp actor admin state passive`
Mode	Interface Config

lacp actor admin state

Use this command to configure the administrative value of actor state as transmitted by the Actor in LACPDUs. This command can be used to configure a single interfaces or a range of interfaces.

Default	0x07
Format	`lacp actor admin state {individual|longtimeout|passive}`
Mode	Interface Config

Note
This command is applicable only to physical interfaces.

no lacp actor admin state

Use this command the configure the default administrative values of actor state as transmitted by the Actor in LACPDUs.

Note
Both the `no portlacptimeout` and the `no lacp actor admin state` commands set the values back to default, regardless of the command used to configure the ports. Consequently, both commands will display in `show running-config`.

Format	`no lacp actor admin state {individual|longtimeout|passive}`
Mode	Interface Config

lacp actor port priority

Use this command to configure the priority value assigned to the Aggregation Port for an interface or range of interfaces. The valid range for *`priority`* is 0 to 65535.

Default	0x80
Format	`lacp actor port priority` *`0-65535`*
Mode	Interface Config

Note
This command is applicable only to physical interfaces.

no lacp actor port priority

Use this command to configure the default priority value assigned to the Aggregation Port.

Format	`no lacp actor port priority`
Mode	Interface Config

lacp partner admin key

Use this command to configure the administrative value of the Key for the protocol partner. This command can be used to configure a single interface or a range of interfaces. The valid range for *key* is 0 to 65535.

Default	0x0
Format	`lacp partner admin key` *key*
Mode	Interface Config

Note
This command is applicable only to physical interfaces.

no lacp partner admin key

Use this command to set the administrative value of the Key for the protocol partner to the default.

Format	`no lacp partner admin key`
Mode	Interface Config

lacp partner admin state individual

Use this command to set LACP partner admin state to individual.

Format	`lacp partner admin state individual`
Mode	Interface Config

Note
This command is applicable only to physical interfaces.

no lacp partner admin state individual

Use this command to set the LACP partner admin state to aggregation.

Format	`no lacp partner admin state individual`
Mode	Interface Config

lacp partner admin state longtimeout

Use this command to set LACP partner admin state to longtimeout.

Format	`lacp partner admin state longtimeout`
Mode	Interface Config

Note
This command is applicable only to physical interfaces.

no lacp partner admin state longtimeout

Use this command to set the LACP partner admin state to short timeout.

Format	`no lacp partner admin state longtimeout`
Mode	Interface Config

Note
This command is applicable only to physical interfaces.

lacp partner admin state passive

Use this command to set the LACP partner admin state to passive.

Format	`lacp partner admin state passive`
Mode	Interface Config

Note
This command is applicable only to physical interfaces.

no lacp partner admin state passive

Use this command to set the LACP partner admin state to active.

Format	`no lacp partner admin state passive`
Mode	Interface Config

lacp partner port id

Use this command to configure the LACP partner port id. This command can be used to configure a single interface or a range of interfaces. The valid range for *`port-id`* is 0 to 65535.

Default	0x80
Format	`lacp partner port-id` *`port-id`*
Mode	Interface Config

Note
This command is applicable only to physical interfaces.

no lacp partner port id

Use this command to set the LACP partner port id to the default.

Format	`no lacp partner port-id`
Mode	Interface Config

lacp partner port priority

Use this command to configure the LACP partner port priority. This command can be used to configure a single interface or a range of interfaces. The valid range for *`priority`* is 0 to 65535.

Default	0x0
Format	`lacp partner port priority` *`priority`*
Mode	Interface Config

Note
This command is applicable only to physical interfaces.

no lacp partner port priority

Use this command to configure the default LACP partner port priority.

Format	`no lacp partner port priority`
Mode	Interface Config

lacp partner system-id

Use this command to configure the 6-octet MAC Address value representing the administrative value of the Aggregation Port's protocol Partner's System ID. This command can be used to configure a single interface or a range of interfaces. The valid range of *`system-id`* is 00:00:00:00:00:00 - FF:FF:FF:FF:FF:FF.

Default	00:00:00:00:00:00
Format	`lacp partner system-id` *`system-id`*
Mode	Interface Config

Note
This command is applicable only to physical interfaces.

no lacp partner system-id

Use this command to configure the default value representing the administrative value of the Aggregation Port's protocol Partner's System ID.

Format	`no lacp partner system-id`
Mode	Interface Config

lacp partner system priority

Use this command to configure the administrative value of the priority associated with the Partner's System ID. This command can be used to configure a single interface or a range of interfaces. The valid range for *`priority`* is 0 to 65535.

Default	0x0
Format	`lacp partner system priority` *`0-65535`*
Mode	Interface Config

Note
This command is applicable only to physical interfaces.

no lacp partner system priority

Use this command to configure the default administrative value of priority associated with the Partner's System ID.

Format	`no lacp partner system priority`
Mode	Interface Config

interface lag

Use this command to enter Interface configuration mode for the specified LAG.

Format	`interface lag` *`lag-interface-number`*
Mode	Global Config

port-channel static

This command enables the static mode on a port-channel (LAG) interface or range of interfaces. By default the static mode for a new port-channel is enabled, which means the port-channel is static. If the maximum number of allowable dynamic port-channels are already present in the system, the static mode for a new port-channel is enabled, which means the port-channel is static. You can only use this command on port-channel interfaces.

Default	enabled
Format	`port-channel static`
Mode	Interface Config

no port-channel static

This command sets the static mode on a particular port-channel (LAG) interface to the default value. This command will be executed only for interfaces of type port-channel (LAG).

Format	`no port-channel static`
Mode	Interface Config

port lacpmode

This command enables Link Aggregation Control Protocol (LACP) on a port or range of ports.

Default	enabled
Format	`port lacpmode`
Mode	Interface Config

no port lacpmode

This command disables Link Aggregation Control Protocol (LACP) on a port.

Format	`no port lacpmode`
Mode	Interface Config

port lacpmode enable all

This command enables Link Aggregation Control Protocol (LACP) on all ports.

Format	`port lacpmode enable all`
Mode	Global Config

no port lacpmode enable all

This command disables Link Aggregation Control Protocol (LACP) on all ports.

Format	`no port lacpmode enable all`
Mode	Global Config

port lacptimeout (Interface Config)

This command sets the timeout on a physical interface or range of interfaces of a particular device type (actor or partner) to either long or short timeout.

Default	long
Format	`port lacptimeout {actor | partner} {long | short}`
Mode	Interface Config

no port lacptimeout

This command sets the timeout back to its default value on a physical interface of a particular device type (actor or partner).

Format	`no port lacptimeout {actor | partner}`
Mode	Interface Config

Note

Both the `no portlacptimeout` and the `no lacp actor admin state` commands set the values back to default, regardless of the command used to configure the ports. Consequently, both commands will display in `show running-config`.

port lacptimeout (Global Config)

This command sets the timeout for all interfaces of a particular device type (actor or partner) to either long or short timeout.

Default	long
Format	`port lacptimeout {actor | partner} {long | short}`
Mode	Global Config

no port lacptimeout

This command sets the timeout for all physical interfaces of a particular device type (actor or partner) back to their default values.

Format	`no port lacptimeout {actor | partner}`
Mode	Global Config

Note

Both the `no portlacptimeout` and the `no lacp actor admin state` commands set the values back to default, regardless of the command used to configure the ports. Consequently, both commands will display in `show running-config`.

port-channel adminmode

This command enables all configured port-channels with the same administrative mode setting.

Format	`port-channel adminmode all`

Mode	Global Config

no port-channel adminmode

This command disables all configured port-channels with the same administrative mode setting.

Format	`no port-channel adminmode all`
Mode	Global Config

port-channel linktrap

This command enables link trap notifications for the port-channel (LAG). The interface is a logical slot/port for a configured port-channel. The option `all` sets every configured port-channel with the same administrative mode setting.

Default	enabled
Format	`port-channel linktrap {`*`logical`* `slot/port | all}`
Mode	Global Config

no port-channel linktrap

This command disables link trap notifications for the port-channel (LAG). The interface is a logical slot and port for a configured port-channel. The option `all` sets every configured port-channel with the same administrative mode setting.

Format	`no port-channel linktrap {`*`logical`* `slot/port | all}`
Mode	Global Config

port-channel load-balance

This command selects the load-balancing option used on a port-channel (LAG). Traffic is balanced on a port-channel (LAG) by selecting one of the links in the channel over which to transmit specific packets. The link is selected by creating a binary pattern from selected fields in a packet, and associating that pattern with a particular link.

Load-balancing is not supported on every device. The range of options for load-balancing may vary per device.

This command can be configured for a single interface, a range of interfaces, or all interfaces. Instead of slot/port, `lag` *`lag-intf-num`* can be used as an alternate way to specify the LAG interface. `lag` *`lag-intf-num`* can also be used to specify the LAG interface where *`lag-intf-num`* is the LAG port number.

Default	3
Format	`port-channel load-balance {1 | 2 | 3 | 4 | 5 | 6 | 7} {slot/port | all}`
Mode	Interface Config Global Config

Term	Definition
1	Source MAC, VLAN, EtherType, and incoming port associated with the packet
2	Destination MAC, VLAN, EtherType, and incoming port associated with the packet
3	Source/Destination MAC, VLAN, EtherType, and incoming port associated with the packet
4	Source IP and Source TCP/UDP fields of the packet
5	Destination IP and Destination TCP/UDP Port fields of the packet
6	Source/Destination IP and source/destination TCP/UDP Port fields of the packet
7	Enhanced hashing mode
slot/port| all	Global Config Mode only: The interface is a logical slot/port number of a configured port-channel. `All` applies the command to all currently configured port-channels.

no port-channel load-balance

This command reverts to the default load balancing configuration.

Format	`no port-channel load-balance {slot/port / all}`

Mode	Interface Config Global Config

Term	Definition
slot/port| all	Global Config Mode only: The interface is a logical slot/port number of a configured port-channel. **All** applies the command to all currently configured port-channels.

port-channel min-links

This command configures the port-channel's minimum links for lag interfaces.

Default	`1`
Format	`port-channel min-links` *`1-8`*
Mode	Interface Config

port-channel name

This command defines a name for the port-channel (LAG). The interface is a logical slot/port for a configured port-channel, and *`name`* is an alphanumeric string up to 15 characters.

Format	`port-channel name {`*`logical`* `slot/port}` *`name`*
Mode	Global Config

port-channel system priority

Use this command to configure port-channel system priority. The valid range of `priority` is 0-65535.

Default	0x8000
Format	`port-channel system priority` *`priority`*
Mode	Global Config

no port-channel system priority

Use this command to configure the default port-channel system priority value.

Format	`no port-channel system priority`
Mode	Global Config

show lacp actor

Use this command to display LACP actor attributes. Instead of slot/port, `lag` *`lag-intf-num`* can be used as an alternate way to specify the LAG interface. `lag` *`lag-intf-num`* can also be used to specify the LAG interface where *`lag-intf-num`* is the LAG port number.

Format	`show lacp actor {slot/port|all}`
Mode	Global Config

The following output parameters are displayed.

Parameter	Description
System Priority	The administrative value of the Key.
Actor Admin Key	The administrative value of the Key.
Port Priority	The priority value assigned to the Aggregation Port.
Admin State	The administrative values of the actor state as transmitted by the Actor in LACPDUs.

show lacp partner

Use this command to display LACP partner attributes.

Format	`show lacp actor {slot/port|all}`
Mode	Privileged EXEC

The following output parameters are displayed.

Parameter	Description
System Priority	The administrative value of priority associated with the Partner's System ID.

Parameter	Description
System-ID	Represents the administrative value of the Aggregation Port's protocol Partner's System ID.
Admin Key	The administrative value of the Key for the protocol Partner.
Port Priority	The administrative value of the Key for protocol Partner.
Port-ID	The administrative value of the port number for the protocol Partner.
Admin State	The administrative values of the actor state for the protocol Partner.

show port-channel brief

This command displays the static capability of all port-channel (LAG) interfaces on the device as well as a summary of individual port-channel interfaces.

Format	`show port-channel brief`
Mode	User EXEC

For each port-channel the following information is displayed:

Term	Definition
Logical Interface	The slot/port of the logical interface.
Port-channel Name	The name of port-channel (LAG) interface.
Link-State	Shows whether the link is up or down.
Trap Flag	Shows whether trap flags are enabled or disabled.
Type	Shows whether the port-channel is statically or dynamically maintained.
Mbr Ports	The members of this port-channel.
Active Ports	The ports that are actively participating in the port-channel.

show port-channel

This command displays an overview of all port-channels (LAGs) on the switch. Instead of slot/port, `lag` *`lag-intf-num`* can be used as an alternate way to specify the LAG interface. `lag` *`lag-intf-num`* can also be used to specify the LAG interface where *`lag-intf-num`* is the LAG port number.

Format	`show port-channel`
Mode	Privileged EXEC

Term	Definition
Logical Interface	The valid slot/port number.
Port-Channel Name	The name of this port-channel (LAG). You may enter any string of up to 15 alphanumeric characters.
Link State	Indicates whether the Link is up or down.
Admin Mode	May be enabled or disabled. The factory default is enabled.
Type	The status designating whether a particular port-channel (LAG) is statically or dynamically maintained. ◆ **Static** - The port-channel is statically maintained. ◆ **Dynamic** - The port-channel is dynamically maintained.
Load Balance Option	The load balance option associated with this LAG. See “port-channel load-balance” on page 457.
Local Preference Mode	Indicates whether the local preference mode is **enabled** or **disabled**.
Mbr Ports	A listing of the ports that are members of this port-channel (LAG), in slot/port notation. There can be a maximum of eight ports assigned to a given port-channel (LAG).
Device Timeout	For each port, lists the timeout (**long** or **short**) for Device Type (**actor** or **partner**).

Term	Definition
Port Speed	Speed of the port-channel port.
Active Ports	This field lists ports that are actively participating in the port-channel (LAG).

The following shows example CLI display output for the command.

```
(CN1610) #show port-channel 0/3/1


Local Interface.............................. 0/3/1
Channel Name................................. ch1
Link State................................... Up
Admin Mode................................... Enabled
Type......................................... Static
Load Balance Option.......................... 3
(Src/Dest MAC, VLAN, EType, incoming port)
Local Preference Mode........................ Enabled

Mbr    Device/       Port      Port
Ports  Timeout       Speed     Active
------ ------------- --------- -------
1/0/1  actor/long    Auto      True
       partner/long
1/0/2  actor/long    Auto      True
       partner/long
1/0/3  actor/long    Auto      False
       partner/long
1/0/4  actor/long    Auto      False
       partner/long
```

show port-channel system priority

Use this command to display the port-channel system priority.

Format	`show port-channel system priority`
Mode	Privileged EXEC

show port-channel counters

Use this command to display port-channel counters for the specified port.

Format	`show port-channel slot/port counters`

Mode	Privileged EXEC

Term	Definition
Local Interface	The valid slot/port number.
Channel Name	The name of this port-channel (LAG).
Link State	Indicates whether the Link is up or down.
Admin Mode	May be enabled or disabled. The factory default is enabled.
Port Channel Flap Count	The number of times the port-channel was inactive.
Mbr Ports	The slot/port for the port member.
Mbr Flap Counters	The number of times a port member is inactive, either because the link is down, or the admin state is disabled.

The following shows example CLI display output for the command.

```
(CN1610) #show port-channel 3/1 counters


Local Interface.............................. 3/1
Channel Name................................. ch1
Link State................................... Down
Admin Mode................................... Enabled
Port Channel Flap Count...................... 0

Mbr    Mbr Flap
Ports  Counters
------ ---------
0/1    0
0/2    0
0/3    1
0/4    0
0/5    0
0/6    0
0/7    0
0/8    0
```

clear port-channel counters

Use this command to clear and reset specified port-channel and member flap counters for the specified interface.

Format	`clear port-channel {lag-intf-num | slot/port} counters`
Mode	Privileged EXEC

clear port-channel all counters

Use this command to clear and reset all port-channel and member flap counters for the specified interface.

Format	`clear port-channel all counters`
Mode	Privileged EXEC

Port Mirroring Commands

Port mirroring, which is also known as port monitoring, selects network traffic that you can analyze with a network analyzer, such as a SwitchProbe device or other Remote Monitoring (RMON) probe.

monitor session

This command configures a probe port and a monitored port for monitor session (port monitoring). Use the `source interface` slot/port parameter to specify the interface to monitor. Use `rx` to monitor only ingress packets, or use *`tx`* to monitor only egress packets. If you do not specify an `{rx | tx}` option, the destination port monitors both ingress and egress packets.

A VLAN can be configured as the source to a session (all member ports of that VLAN are monitored). Remote port mirroring is configured by adding the RSPAN VLAN ID. At the source switch, the destination is configured as the RSPAN VLAN and at the destination switch, the source is configured as the RSPAN VLAN.

Note
The source and destination cannot be configured as remote on the same device.

The `reflector-port` is configured at the source switch. The `reflector-port` forwards the mirrored traffic towards the destination switch.

Note
This port must be configured with RSPAN VLAN membership.

IP/MAC ACL can be attached to a session by giving the access list number/name.

Use the `destination interface` slot/port to specify the interface to receive the monitored traffic.

Use the *`mode`* parameter to enable the administrative mode of the session. If enabled, the probe port monitors all the traffic received and transmitted on the physical monitored port.

Use the filter parameter to filter a specified access group either by IP address or MAC address.

Format	monitor session *session-id* {source {interface slot/port | vlan *vlan-id* | remote vlan *vlan-id* }[{rx | tx}] | destination {interface slot/port |remote vlan *vlan-id* reflector-port *unit/slot/port*}| mode | filter {ip access-group *acl-id/aclname* |mac access-group *acl-name*}}
Mode	Global Config

To configure the RSPAN VLAN source:
monitor session *session-id* source {interface *unit/slot/port* | vlan *vlan-id* | remote vlan *vlan-id* }[rx/tx]

To the configure RSPAN VLAN destination:
monitor session *session-id* destination {interface *unit/slot/port* |remote vlan *vlan-id* reflector-port *unit/slot/port*}

To attach an ACL:
monitor session *session-id* filter {ip access-group *acl-id/aclname* |mac access-group *acl-name*}

no monitor session

Use this command without optional parameters to remove the monitor session (port monitoring) designation from the source probe port, the destination monitored port and all VLANs. Once the port is removed from the VLAN, you must manually add the port to any desired VLANs. Use the source interface slot/port parameter or destination interface to remove the specified interface from the port monitoring session. Use the mode parameter to disable the administrative mode of the session

Note
Since the current version of FASTPATH software only supports one session, if you do not supply optional parameters, the behavior of this command is similar to the behavior of the no monitor command.

Format	no monitor session *session-id* [{source interface slot/port | destination interface | mode |filter {ip access-group |mac access-group}}]
Mode	Global Config

no monitor

This command removes all the source ports and a destination port for the and restores the default value for mirroring session mode for all the configured sessions.

Note
This is a stand-alone "no" command. This command does not have a "normal" form.

Default	enabled
Format	`no monitor`
Mode	Global Config

show monitor session

This command displays the Port monitoring information for a particular mirroring session.

The *session-id* parameter is an integer value used to identify the session and ranges from 1–4.

Format	`show monitor session` *session-id*
Mode	Privileged EXEC

Term	Definition
Session ID	An integer value used to identify the session. Its value can be anything between 1 and the maximum number of mirroring sessions allowed on the platform.
Monitor Session Mode	Indicates whether the Port Mirroring feature is enabled or disabled for the session identified with *session-id*. The possible values are Enabled and Disabled.
Probe Port	Probe port (destination port) for the session identified with *session-id*. If probe port is not set then this field is blank.

Term	Definition
Source Port	The port, which is configured as mirrored port (source port) for the session identified with *session-id*. If no source port is configured for the session then this field is blank.
Type	Direction in which source port configured for port mirroring.Types are tx for transmitted packets and rx for receiving packets.
Src VLAN	All member ports of this VLAN are mirrored. If the source VLAN is not configured, this field is blank.
Ref. Port	This port carries all the mirrored traffic at the source switch.
Src Remote VLAN	The source VLAN is configured at the destination switch. If the remote VLAN is not configured, this field is blank.
Dst Remote VLAN	The destination VLAN is configured at the source switch. If the remote VLAN is not configured, this field is blank.
IP ACL	The IP access-list id or name attached to the port mirroring session.
MAC ACL	The MAC access-list name attached to the port mirroring session.

show vlan remote-span

This command displays the configured RSPAN VLAN.

Format	`show vlan remote-span`
Mode	Privileged EXEC Mode

The following shows example output for the command.

```
(CN1610)# show vlan remote-span

Remote SPAN VLAN
-----------------------------------------------------------------
------
```

```
100
```

Static MAC Filtering Commands

The commands in this section describe how to configure static MAC filtering. Static MAC filtering allows you to configure destination ports for a static multicast MAC filter irrespective of the platform.

macfilter

This command adds a static MAC filter entry for the MAC address *macaddr* on the VLAN *vlanid*. The value of the *macaddr* parameter is a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6. The restricted MAC Addresses are: 00:00:00:00:00:00, 01:80:C2:00:00:00 to 01:80:C2:00:00:0F, 01:80:C2:00:00:20 to 01:80:C2:00:00:21, and FF:FF:FF:FF:FF:FF. The *vlanid* parameter must identify a valid VLAN.

The number of static mac filters supported on the system is different for MAC filters where source ports are configured and MAC filters where destination ports are configured.

- For unicast MAC address filters and multicast MAC address filters with source port lists, the maximum number of static MAC filters supported is 20.
- For multicast MAC address filters with destination ports configured, the maximum number of static filters supported is 256.

i.e. For current Broadcom platforms, you can configure the following combinations:

- Unicast MAC and source port (max = 20)
- Multicast MAC and source port (max = 20)
- Multicast MAC and destination port (only) (max = 256)
- Multicast MAC and source ports and destination ports (max = 20)

Format	`macfilter macaddr vlanid`
Mode	Global Config

no macfilter

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

The *vlanid* parameter must identify a valid VLAN.

Format	`no macfilter` *`macaddr vlanid`*
Mode	Global Config

macfilter adddest

Use this command to add the interface or range of interfaces to the destination filter set for the MAC filter with the given *macaddr* and VLAN of *vlanid*. The *macaddr* parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6. The *vlanid* parameter must identify a valid VLAN.

Note
Configuring a destination port list is only valid for multicast MAC addresses.

Format	`macfilter adddest` *`macaddr`*
Mode	Interface Config

no macfilter adddest

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

Format	`no macfilter adddest` *`macaddr`*
Mode	Interface Config

macfilter adddest all

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

Note
Configuring a destination port list is only valid for multicast MAC addresses.

Format	`macfilter adddest all` *`macaddr`*

Mode	Global Config

no macfilter adddest all

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

Format	`no macfilter adddest all` *macaddr*
Mode	Global Config

macfilter addsrc

This command adds the interface or range of interfaces to the source filter set for the MAC filter with the MAC address of *macaddr* and VLAN of *vlanid*. The *macaddr* parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6. The *vlanid* parameter must identify a valid VLAN.

Format	`macfilter addsrc` *macaddr vlanid*
Mode	Interface Config

no macfilter addsrc

This command removes a port from the source filter set for the MAC filter with the MAC address of *macaddr* and VLAN of *vlanid*. The *macaddr* parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6. The *vlanid* parameter must identify a valid VLAN.

Format	`no macfilter addsrc` *macaddr vlanid*
Mode	Interface Config

macfilter addsrc all

This command adds all interfaces to the source filter set for the MAC filter with the MAC address of *macaddr* and *vlanid*. You must specify the *macaddr* parameter as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6. The *vlanid* parameter must identify a valid VLAN.

Format	`macfilter addsrc all` *macaddr vlanid*

Mode	Global Config

no macfilter addsrc all

This command removes all interfaces to the source filter set for the MAC filter with the MAC address of *macaddr* and VLAN of *vlanid*. You must specify the *macaddr* parameter as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6.

The *vlanid* parameter must identify a valid VLAN.

Format	`no macfilter addsrc all` *macaddr vlanid*
Mode	Global Config

show mac-address-table static

This command displays the Static MAC Filtering information for all Static MAC Filters. If you specify `all`, all the Static MAC Filters in the system are displayed. If you supply a value for *macaddr*, you must also enter a value for *vlanid*, and the system displays Static MAC Filter information only for that MAC address and VLAN.

Format	`show mac-address-table static {`*macaddr vlanid* `| all}`
Mode	Privileged EXEC

Term	Definition
MAC Address	The MAC Address of the static MAC filter entry.
VLAN ID	The VLAN ID of the static MAC filter entry.
Source Port(s)	The source port filter set's slot and port(s).

Note

Only multicast address filters will have destination port lists.

show mac-address-table staticfiltering

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

Format	`show mac-address-table staticfiltering`
Mode	Privileged EXEC

Term	Definition
VLAN ID	The VLAN in which the MAC Address is learned.
MAC Address	A unicast MAC address for which the switch has forwarding and or filtering information. As the data is gleaned from the MFDB, the address will be a multicast address. The format is 6 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB.
Type	The type of the entry. Static entries are those that are configured by the end user. Dynamic entries are added to the table as a result of a learning process or protocol.
Description	The text description of this multicast table entry.
Interfaces	The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).

DHCP L2 Relay Agent Commands

You can enable the switch to operate as a DHCP Layer 2 relay agent to relay DHCP requests from clients to a Layer 3 relay agent or server. The Circuit ID and Remote ID can be added to DHCP requests relayed from clients to a DHCP server. This information is included in DHCP Option 82, as specified in sections 3.1 and 3.2 of RFC3046.

dhcp l2relay

This command enables the DHCP Layer 2 Relay agent for an interface a range of interfaces in, or all interfaces. The subsequent commands mentioned in this section can only be used when the DHCP L2 relay is enabled.

Format	`dhcp l2relay`
Mode	◆ Global Config ◆ Interface Config

no dhcp l2relay

This command disables DHCP Layer 2 relay agent for an interface or range of interfaces.

Format	`no dhcp l2relay`
Mode	◆ Global Config ◆ Interface Config

dhcp l2relay circuit-id subscription

This command sets the Option-82 Circuit ID for a given service subscription identified by *`subscription-string`* on a given interface. The *`subscription-string`* is a character string which needs to be matched with a configured DOT1AD subscription string for correct operation. When circuit-id is enabled using this command, all Client DHCP requests that fall under this service subscription are added with Option-82 circuit-id as the incoming interface number.

Default	disabled
Format	`dhcp l2relay circuit-id subscription subscription-string`

Mode	Interface Config

no dhcp l2relay circuit-id subscription

This command resets the Option-82 Circuit ID for a given service subscription identified by *subscription-string* on a given interface. The *subscription-string* is a character string which needs to be matched with a configured DOT1AD subscription string for correct operation. When circuit-id is disabled using this command, all Client DHCP requests that fall under this service subscription are no longer added with Option-82 circuit-id.

Format	`no dhcp l2relay circuit-id subscription` *subscription-string*
Mode	Interface Config

dhcp l2relay circuit-id vlan

This parameter sets the DHCP Option-82 Circuit ID for a VLAN. When enabled, the interface number is added as the Circuit ID in DHCP option 82.

Format	`dhcp l2relay circuit-id vlan` *vlan-list*
Mode	Global Config

Parameter	Description
vlan–list	The VLAN ID. The range is 1–4093. Separate nonconsecutive IDs with a comma (,) no spaces and no zeros in between the range. Use a dash (–) for the range.

no dhcp l2relay circuit-id vlan

This parameter clears the DHCP Option-82 Circuit ID for a VLAN.

Format	`no dhcp l2relay circuit-id vlan` *vlan-list*
Mode	Global Config

dhcp l2relay remote-id subscription

This command sets the Option-82 Remote-ID string for a given service subscription identified by *subscription-string* on a given interface or range of interfaces. The *subscription-string* is a character string which needs to be matched with a configured DOT1AD subscription string for correct operation. The *remoteid-string* is a character string. When remote-id string is set using this command, all Client DHCP requests that fall under this service subscription are added with Option-82 Remote-id as the configured remote-id string.

Default	empty string
Format	`dhcp l2relay remote-id` *`remoteid-string`* `subscription-name` *`subscription-string`*
Mode	Interface Config

no dhcp l2relay remote-id subscription

This command resets the Option-82 Remote-ID string for a given service subscription identified by *subscription-string* on a given interface. The *subscription-string* is a character string which needs to be matched with a configured DOT1AD subscription string for correct operation. When remote-id string is reset using this command, the Client DHCP requests that fall under this service subscription are not added with Option-82 Remote-id.

Format	`no dhcp l2relay remote-id` *`remoteid-string`* `subscription-name` *`subscription-string`*
Mode	Interface Config

dhcp l2relay remote-id vlan

This parameter sets the DHCP Option-82 Remote ID for a VLAN and subscribed service (based on subscription-name).

Format	`dhcp l2relay remote-id` *`remote-id-string`* `vlan` *`vlan-list`*
Mode	Global Config

Parameter	Description
vlan–list	The VLAN ID. The range is 1–4093. Separate nonconsecutive IDs with a comma (,) no spaces and no zeros in between the range. Use a dash (–) for the range.

no dhcp l2relay remote-id vlan

This parameter clears the DHCP Option-82 Remote ID for a VLAN and subscribed service (based on subscription-name).

Format	`no dhcp l2relay remote-id vlan` *`vlan-list`*
Mode	Global Config

dhcp l2relay trust

Use this command to configure an interface or range of interfaces as trusted for Option-82 reception.

Default	untrusted
Format	`dhcp l2relay trust`
Mode	Interface Config

no dhcp l2relay trust

Use this command to configure an interface to the default untrusted for Option-82 reception.

Format	`no dhcp l2relay trust`
Mode	Interface Config

dhcp l2relay vlan

Use this command to enable the DHCP L2 Relay agent for a set of VLANs. All DHCP packets which arrive on interfaces in the configured VLAN are subject to L2 Relay processing.

Default	`disable`

Format	`dhcp l2relay vlan vlan-list`
Mode	Global Config

Parameter	Description
vlan–list	The VLAN ID. The range is 1–4093. Separate nonconsecutive IDs with a comma (,) no spaces and no zeros in between the range. Use a dash (–) for the range.

no dhcp l2relay vlan

Use this command to disable the DHCP L2 Relay agent for a set of VLANs.

Format	`no dhcp l2relay vlan vlan-list`
Mode	Global Config

show dhcp l2relay all

This command displays the summary of DHCP L2 Relay configuration.

Format	`show dhcp l2relay all`
Mode	Privileged EXEC

The following shows example CLI display output for the command.

```
(Broadcom FASTPATH Switching) #show dhcp l2relay all

DHCP L2 Relay is Enabled.

Interface  L2RelayMode   TrustMode
---------  -----------  --------------
 0/2        Enabled      untrusted
 0/4        Disabled     trusted

VLAN Id    L2 Relay  CircuitId  RemoteId
-------- ----------  ----------- ------------
 3           Disabled    Enabled    --NULL--
5           Enabled     Enabled    --NULL--
 6           Enabled     Enabled    broadcom
 7           Enabled     Disabled   --NULL--
```

```
8           Enabled     Disabled   --NULL--
9           Enabled     Disabled   --NULL--
10          Enabled     Disabled   --NULL--
```

show dhcp l2relay circuit-id vlan

This command displays DHCP circuit-id vlan configuration.

Format	`show dhcp l2relay circuit-id vlan` *vlan-list*
Mode	Privileged EXEC

Parameter	Description
vlan-list	Enter VLAN IDs in the range 1–4093. Use a dash (–) to specify a range or a comma (,) to separate VLAN IDs in a list. Spaces and zeros are not permitted.

show dhcp l2relay interface

This command displays DHCP L2 relay configuration specific to interfaces.

Format	`show dhcp l2relay interface {all |` *interface-num*`}`
Mode	Privileged EXEC

The following shows example CLI display output for the command.

```
(Broadcom FASTPATH Switching) #show dhcp l2relay interface all

DHCP L2 Relay is  Enabled.

Interface  L2RelayMode   TrustMode
---------  -----------  --------------
 0/2        Enabled      untrusted
 0/4        Disabled     trusted
```

show dhcp l2relay remote-id vlan

This command displays DHCP Remote-id vlan configuration.

Format	`show dhcp l2relay remote-id vlan` *vlan-list*
Mode	Privileged EXEC

Parameter	Description
vlan-list	Enter VLAN IDs in the range 1–4093. Use a dash (–) to specify a range or a comma (,) to separate VLAN IDs in a list. Spaces and zeros are not permitted.

show dhcp l2relay stats interface

This command displays statistics specific to DHCP L2 Relay configured interface.

Format	`show dhcp l2relay stats interface {all | interface-num}`
Mode	Privileged EXEC

The following shows example CLI display output for the command.

```
(Broadcom FASTPATH Switching) #show dhcp l2relay stats interface
all

DHCP L2 Relay is  Enabled.

Interface  UntrustedServer    UntrustedClient  TrustedServer
TrustedClient
            MsgsWithOpt82    MsgsWithOpt82    MsgsWithoutOpt82
MsgsWithoutOpt82
---------  --------------- -----------------  ----------------- ---
-----------
 0/1           0                 0                 0                0
 0/2           0                 0                 3                7
 0/3           0                 0                 0                0
 0/4           0                 12                0                0
 0/5           0                 0                 0                0
 0/6            3                  0                   0   0
 0/7           0                 0                 0                0
 0/8           0                 0                 0                0
 0/9           0                 0                 0                0
```

show dhcp l2relay agent-option vlan

This command displays the DHCP L2 Relay Option-82 configuration specific to VLAN.

Format	show dhcp l2relay agent-option vlan *vlan-range*
Mode	Privileged EXEC

The following shows example CLI display output for the command.

```
(Broadcom FASTPATH Switching) #show dhcp l2relay agent-option vlan
5-10

DHCP L2 Relay is  Enabled.

VLAN Id    L2 Relay  CircuitId  RemoteId
--------- ----------  ---------- ------------
5           Enabled     Enabled    --NULL--
6           Enabled     Enabled    broadcom
7           Enabled     Disabled   --NULL--
8           Enabled     Disabled   --NULL--
9           Enabled     Disabled   --NULL--
10          Enabled     Disabled   --NULL--
```

show dhcp l2relay vlan

This command displays DHCP vlan configuration.

Format	show dhcp l2relay vlan *vlan-list*
Mode	Privileged EXEC

Parameter	Description
vlan-list	Enter VLAN IDs in the range 1–4093. Use a dash (–) to specify a range or a comma (,) to separate VLAN IDs in a list. Spaces and zeros are not permitted.

clear dhcp l2relay statistics interface

Use this command to reset the DHCP L2 relay counters to zero. Specify the port with the counters to clear, or use the `all` keyword to clear the counters on all ports.

Format	clear dhcp l2relay statistics interface {slot/port | *all*}

Mode	Privileged EXEC

DHCP Client Commands

FASTPATH can include vendor and configuration information in DHCP client requests relayed to a DHCP server. This information is included in DHCP Option 60, Vendor Class Identifier. The information is a string of 128 octets.

dhcp client vendor-id-option

This command enables the inclusion of DHCP Option-60, Vendor Class Identifier included in the requests transmitted to the DHCP server by the DHCP client operating in the FASTPATH switch.

Format	`dhcp client vendor-id-option` *`string`*
Mode	Global Config

no dhcp client vendor-id-option

This command disables the inclusion of DHCP Option-60, Vendor Class Identifier included in the requests transmitted to the DHCP server by the DHCP client operating in the FASTPATH switch.

Format	`no dhcp client vendor-id-option`
Mode	Global Config

dhcp client vendor-id-option-string

This parameter sets the DHCP Vendor Option-60 string to be included in the requests transmitted to the DHCP server by the DHCP client operating in the FASTPATH switch.

Format	`dhcp client vendor-id-option-string` *`string`*
Mode	Global Config

no dhcp client vendor-id-option-string

This parameter clears the DHCP Vendor Option-60 string.

Format	`no dhcp client vendor-id-option-string`
Mode	Global Config

show dhcp client vendor-id-option

This command displays the configured administration mode of the vendor-id-option and the vendor-id string to be included in Option-43 in DHCP requests.

Format	`show dhcp client vendor-id-option`
Mode	Privileged EXEC

The following shows example CLI display output for the command.

```
(Broadcom FASTPATH Switching) #show dhcp client vendor-id-option

DHCP Client Vendor Identifier Option is Enabled
DHCP Client Vendor Identifier Option string is FastpathClient.
```

DHCP Snooping Configuration Commands

This section describes commands you use to configure DHCP Snooping.

ip dhcp snooping

Use this command to enable DHCP Snooping globally.

Default	disabled
Format	`ip dhcp snooping`
Mode	Global Config

no ip dhcp snooping

Use this command to disable DHCP Snooping globally.

Format	`no ip dhcp snooping`
Mode	Global Config

ip dhcp snooping vlan

Use this command to enable DHCP Snooping on a list of comma-separated VLAN ranges.

Default	disabled
Format	`ip dhcp snooping vlan` *`vlan-list`*
Mode	Global Config

no ip dhcp snooping vlan

Use this command to disable DHCP Snooping on VLANs.

Format	`no ip dhcp snooping vlan` *`vlan-list`*
Mode	Global Config

ip dhcp snooping verify mac-address

Use this command to enable verification of the source MAC address with the client hardware address in the received DCHP message.

Default	enabled
Format	`ip dhcp snooping verify mac-address`
Mode	Global Config

no ip dhcp snooping verify mac-address

Use this command to disable verification of the source MAC address with the client hardware address.

Format	`no ip dhcp snooping verify mac-address`
Mode	Global Config

ip dhcp snooping database

Use this command to configure the persistent location of the DHCP Snooping database. This can be local or a remote file on a given IP machine.

Default	local
Format	`ip dhcp snooping database {local|tftp://hostIP/filename}`
Mode	Global Config

ip dhcp snooping database write-delay

Use this command to configure the interval in seconds at which the DHCP Snooping database will be persisted. The interval value ranges from 15 to 86400 seconds.

Default	300 seconds
Format	`ip dhcp snooping database write-delay in seconds`
Mode	Global Config

no ip dhcp snooping database write-delay

Use this command to set the write delay value to the default value.

Format	`no ip dhcp snooping database write-delay`

Mode	Global Config

ip dhcp snooping binding

Use this command to configure static DHCP Snooping binding.

Format	`ip dhcp snooping binding` *`mac-address`* `vlan` *`vlan id ip address`* `interface` *`interface id`*
Mode	Global Config

no ip dhcp snooping binding

Use this command to remove the DHCP static entry from the DHCP Snooping database.

Format	`no ip dhcp snooping binding` *`mac-address`*
Mode	Global Config

ip verify binding

Use this command to configure static IP source guard (IPSG) entries.

Format	`ip verify binding` *`mac-address`* `vlan` *`vlan id ip address`* `interface` *`interface id`*
Mode	Global Config

no ip verify binding

Use this command to remove the IPSG static entry from the IPSG database.

Format	`no ip verify binding` *`mac-address`* `vlan` *`vlan id ip address`* `interface` *`interface id`*
Mode	Global Config

ip dhcp snooping limit

Use this command to control the rate at which the DHCP Snooping messages come on an interface or range of interfaces. By default, rate limiting is disabled. When enabled, the rate can range from 0 to 300 packets per second. The burst level range is 1 to 15 seconds.

Default	disabled (no limit)
Format	`ip dhcp snooping limit {rate pps [burst interval seconds]}`
Mode	Interface Config

no ip dhcp snooping limit

Use this command to set the rate at which the DHCP Snooping messages come, and the burst level, to the defaults.

Format	`no ip dhcp snooping limit`
Mode	Interface Config

ip dhcp snooping log-invalid

Use this command to control the logging DHCP messages filtration by the DHCP Snooping application. This command can be used to configure a single interface or a range of interfaces.

Default	disabled
Format	`ip dhcp snooping log-invalid`
Mode	Interface Config

no ip dhcp snooping log-invalid

Use this command to disable the logging DHCP messages filtration by the DHCP Snooping application.

Format	`no ip dhcp snooping log-invalid`
Mode	Interface Config

ip dhcp snooping trust

Use this command to configure an interface or range of interfaces as trusted.

Default	disabled
Format	`ip dhcp snooping trust`

Mode	Interface Config

no ip dhcp snooping trust

Use this command to configure the port as untrusted.

Format	`no ip dhcp snooping trust`
Mode	Interface Config

ip verify source

Use this command to configure the IPSG source ID attribute to filter the data traffic in the hardware. Source ID is the combination of IP address and MAC address. Normal command allows data traffic filtration based on the IP address. With the “port-security” option, the data traffic will be filtered based on the IP and MAC addresses.

This command can be used to configure a single interface or a range of interfaces.

Default	`the source ID is the IP address`
Format	`ip verify source {port-security}`
Mode	Interface Config

no ip verify source

Use this command to disable the IPSG configuration in the hardware. You cannot disable port-security alone if it is configured.

Format	`no ip verify source`
Mode	Interface Config

show ip dhcp snooping

Use this command to display the DHCP Snooping global configurations and per port configurations.

Format	`show ip dhcp snooping`
Mode	◆ Privileged EXEC ◆ User EXEC

Term	Definition
Interface	The interface for which data is displayed.
Trusted	If it is enabled, DHCP snooping considers the port as trusted. The factory default is disabled.
Log Invalid Pkts	If it is enabled, DHCP snooping application logs invalid packets on the specified interface.

The following shows example CLI display output for the command.

```
(CN1610) #show ip dhcp snooping

DHCP snooping is Disabled
DHCP snooping source MAC verification is enabled
DHCP snooping is enabled on the following VLANs:
11 - 30, 40

Interface   Trusted    Log Invalid Pkts
---------   --------   ----------------
0/1          Yes             No
0/2          No             Yes
0/3          No             Yes
0/4          No              No
0/6          No              No
```

show ip dhcp snooping binding

Use this command to display the DHCP Snooping binding entries. To restrict the output, use the following options:

- Dynamic: Restrict the output based on DCHP snooping.
- Interface: Restrict the output based on a specific interface.
- Static: Restrict the output based on static entries.
- VLAN: Restrict the output based on VLAN.

Format	`show ip dhcp snooping binding [{static/dynamic}] [interface slot/port] [vlan id]`
Mode	◆ Privileged EXEC ◆ User EXEC

Term	Definition
MAC Address	Displays the MAC address for the binding that was added. The MAC address is the key to the binding database.
IP Address	Displays the valid IP address for the binding rule.
VLAN	The VLAN for the binding rule.
Interface	The interface to add a binding into the DHCP snooping interface.
Type	Binding type; statically configured from the CLI or dynamically learned.
Lease (sec)	The remaining lease time for the entry.

The following shows example CLI display output for the command.

```
(CN1610) #show ip dhcp snooping binding

Total number of bindings: 2

MAC Address          IP Address   VLAN  Interface  Type  Lease time
(Secs)
------------------  ------------  ----  ---------  ---- -----------
-------
00:02:B3:06:60:80   210.1.1.3      10   0/1    86400
00:0F:FE:00:13:04   210.1.1.4      10   0/1      86400
```

show ip dhcp snooping database

Use this command to display the DHCP Snooping configuration related to the database persistency.

Format	`show ip dhcp snooping database`
Mode	◆ Privileged EXEC ◆ User EXEC

Term	Definition
Agent URL	Bindings database agent URL.

Term	Definition
Write Delay	The maximum write time to write the database into local or remote.

The following shows example CLI display output for the command.

```
(CN1610) #show ip dhcp snooping database

agent url:  /10.131.13.79:/sai1.txt

write-delay:  5000
```

show ip dhcp snooping interfaces

Use this command to show the DHCP Snooping status of the interfaces.

Format	show ip dhcp snooping interfaces
Mode	Privileged EXEC

The following shows example CLI display output for the command.

```
(CN1610) #show ip dhcp snooping interfaces

 Interface    Trust State Rate LimitBurst Interval
(pps) (seconds)
-----------   ----------   ----------   --------------
1/g1No151
1/g2No151
1/g3No151

(CN1610) #show ip dhcp snooping interfaces ethernet 1/g15

 Interface    Trust State Rate LimitBurst Interval
(pps) (seconds)
-----------   ----------   ----------   --------------
1/g15Yes151
```

show ip dhcp snooping statistics

Use this command to list statistics for DHCP Snooping security violations on untrusted ports.

Format	show ip dhcp snooping statistics

Mode	◆ Privileged EXEC ◆ User EXEC

Term	Definition
Interface	The IP address of the interface in slot/port format.
MAC Verify Failures	Represents the number of DHCP messages that were filtered on an untrusted interface because of source MAC address and client HW address mismatch.
Client Ifc Mismatch	Represents the number of DHCP release and Deny messages received on the different ports than learned previously.
DHCP Server Msgs Rec'd	Represents the number of DHCP server messages received on Untrusted ports.

The following shows example CLI display output for the command.

```
(CN1610) #show ip dhcp snooping statistics

 Interface    MAC Verify   Client Ifc   DHCP Server
               Failures     Mismatch    Msgs Rec'd
-----------   ----------   ----------   -----------
1/0/2                  0            0             0
1/0/3                  0            0             0
1/0/4                  0            0             0
1/0/5                  0            0             0
1/0/6                  0            0             0
1/0/7                  0            0             0
1/0/8                  0            0             0
1/0/9                  0            0             0
1/0/10                 0            0             0
1/0/11                 0            0             0
1/0/12                 0            0             0
1/0/13                 0            0             0
1/0/14                 0            0             0
1/0/15                 0            0             0
1/0/16                 0            0             0
1/0/17                 0            0             0
1/0/18                 0            0             0
1/0/19                 0            0             0
1/0/20                 0            0             0
```

clear ip dhcp snooping binding

Use this command to clear all DHCP Snooping bindings on all interfaces or on a specific interface.

Format	`clear ip dhcp snooping binding [interface slot/port]`
Mode	◆ Privileged EXEC ◆ User EXEC

clear ip dhcp snooping statistics

Use this command to clear all DHCP Snooping statistics.

Format	`clear ip dhcp snooping statistics`
Mode	◆ Privileged EXEC ◆ User EXEC

show ip verify source

Use this command to display the IPSG configurations on all ports.

Format	`show ip verify source`
Mode	◆ Privileged EXEC ◆ User EXEC

Term	Definition
Interface	Interface address in slot/port format.
Filter Type	Is one of two values: ◆ ip-mac: User has configured MAC address filtering on this interface. ◆ ip: Only IP address filtering on this interface.
IP Address	IP address of the interface
MAC Address	If MAC address filtering is not configured on the interface, the MAC Address field is empty. If port security is disabled on the interface, then the MAC Address field displays “permit-all.”

Term	Definition
VLAN	The VLAN for the binding rule.

The following shows example CLI display output for the command.

```
(CN1610) #show ip verify source

Interface  Filter Type    IP Address       MAC Address       Vlan
---------  -----------  ---------------  -----------------  -----
    0/1     ip-mac       210.1.1.3       00:02:B3:06:60:80     10
    0/1     ip-mac       210.1.1.4       00:0F:FE:00:13:04     10
```

show ip verify interface

Use this command to display the IPSG filter type for a specific interface.

Format	`show ip verify interface slot/port`
Mode	◆ Privileged EXEC ◆ User EXEC

Term	Definition
Interface	Interface address in slot/port format.
Filter Type	Is one of two values: ◆ ip-mac: User has configured MAC address filtering on this interface. ◆ ip: Only IP address filtering on this interface.

show ip source binding

Use this command to display the IPSG bindings.

Format	`show ip source binding [{dhcp-snooping|static}] [interface slot/port] [vlan id]`
Mode	◆ Privileged EXEC ◆ User EXEC

Term	Definition
MAC Address	The MAC address for the entry that is added.
IP Address	The IP address of the entry that is added.
Type	Entry type; statically configured from CLI or dynamically learned from DHCP Snooping.
VLAN	VLAN for the entry.
Interface	IP address of the interface in slot/port format.

The following shows example CLI display output for the command.

```
(CN1610) #show ip source binding

MAC Address       IP Address       Type         Vlan     Interface
----------------  ---------------  -------------  -----  ---------
----
00:00:00:00:00:08         1.2.3.4  dhcp-snooping     2        1/0/1
00:00:00:00:00:09         1.2.3.4  dhcp-snooping     3        1/0/1
00:00:00:00:00:0A         1.2.3.4  dhcp-snooping     4        1/0/1
```

Dynamic ARP Inspection Commands

Dynamic ARP Inspection (DAI) is a security feature that rejects invalid and malicious ARP packets. DAI prevents a class of man-in-the-middle attacks, where an unfriendly station intercepts traffic for other stations by poisoning the ARP caches of its unsuspecting neighbors. The miscreant sends ARP requests or responses mapping another station's IP address to its own MAC address.

DAI relies on DHCP snooping. DHCP snooping listens to DHCP message exchanges and builds a binding database of valid {MAC address, IP address, VLAN, and interface} tuples.

When DAI is enabled, the switch drops ARP packets whose sender MAC address and sender IP address do not match an entry in the DHCP snooping bindings database. You can optionally configure additional ARP packet validation.

ip arp inspection vlan

Use this command to enable Dynamic ARP Inspection on a list of comma-separated VLAN ranges.

Default	`disabled`
Format	`ip arp inspection vlan vlan-list`
Mode	Global Config

no ip arp inspection vlan

Use this command to disable Dynamic ARP Inspection on a list of comma-separated VLAN ranges.

Format	`no ip arp inspection vlan vlan-list`
Mode	Global Config

ip arp inspection validate

Use this command to enable additional validation checks like source-mac validation, destination-mac validation, and ip address validation on the received ARP packets. Each command overrides the configuration of the previous command. For example, if a command enables src-mac and dst-mac validations, and a second command enables IP validation only, the src-mac and dst-mac validations are disabled as a result of the second command.

Default	disabled
Format	ip arp inspection validate {[src-mac] [dst-mac] [ip]}
Mode	Global Config

no ip arp inspection validate

Use this command to disable the additional validation checks on the received ARP packets.

Format	no ip arp inspection validate {[src-mac] [dst-mac] [ip]}
Mode	Global Config

ip arp inspection vlan logging

Use this command to enable logging of invalid ARP packets on a list of comma-separated VLAN ranges.

Default	enabled
Format	ip arp inspection vlan vlan-list logging
Mode	Global Config

no ip arp inspection vlan logging

Use this command to disable logging of invalid ARP packets on a list of comma-separated VLAN ranges.

Format	no ip arp inspection vlan vlan-list logging
Mode	Global Config

ip arp inspection trust

Use this command to configure an interface or range of interfaces as trusted for Dynamic ARP Inspection.

Default	enabled
Format	ip arp inspection trust

Mode	Interface Config

no ip arp inspection trust

Use this command to configure an interface as untrusted for Dynamic ARP Inspection.

Format	`no ip arp inspection trust`
Mode	Interface Config

ip arp inspection limit

Use this command to configure the rate limit and burst interval values for an interface or range of interfaces. Configuring `none` for the limit means the interface is not rate limited for Dynamic ARP Inspections. The maximum pps value shown in the range for the rate option might be more than the hardware allowable limit. Therefore you need to understand the switch performance and configure the maximum rate pps accordingly.

Note
The user interface will accept a rate limit for a trusted interface, but the limit will not be enforced unless the interface is configured to be untrusted.

Default	`15 pps for rate and 1 second for burst-interval`
Format	`ip arp inspection limit {rate pps [burst interval seconds] | none}`
Mode	Interface Config

no ip arp inspection limit

Use this command to set the rate limit and burst interval values for an interface to the default values of 15 pps and 1 second, respectively.

Format	`no ip arp inspection limit`
Mode	Interface Config

ip arp inspection filter

Use this command to configure the ARP ACL used to filter invalid ARP packets on a list of comma-separated VLAN ranges. If the static keyword is given, packets that do not match a permit statement are dropped without consulting the DHCP snooping bindings.

Default	`No ARP ACL is configured on a VLAN`
Format	`ip arp inspection filter acl-name vlan vlan-list [static]`
Mode	Global Config

no ip arp inspection filter

Use this command to unconfigure the ARP ACL used to filter invalid ARP packets on a list of comma-separated VLAN ranges.

Format	`no ip arp inspection filter acl-name vlan vlan-list [static]`
Mode	Global Config

arp access-list

Use this command to create an ARP ACL.

Format	`arp access-list acl-name`
Mode	Global Config

no arp access-list

Use this command to delete a configured ARP ACL.

Format	`no arp access-list acl-name`
Mode	Global Config

permit ip host mac host

Use this command to configure a rule for a valid IP address and MAC address combination used in ARP packet validation.

Format	`permit ip host sender-ip mac host sender-mac`

Mode	ARP Access-list Config

no permit ip host mac host

Use this command to delete a rule for a valid IP and MAC combination.

Format	`no permit ip host sender-ip mac host sender-mac`
Mode	ARP Access-list Config

show ip arp inspection

Use this command to display the Dynamic ARP Inspection global configuration and configuration on all the VLANs. With the *vlan-list* argument (i.e. comma separated VLAN ranges), the command displays the global configuration and configuration on all the VLANs in the given VLAN list. The global configuration includes the **source mac validation**, **destination mac validation** and **invalid IP validation** information.

Format	`show ip arp inspection [vlan vlan-list]`
Mode	◆ Privileged EXEC ◆ User EXEC

Term	Definition
Source MAC Validation	Displays whether Source MAC Validation of ARP frame is enabled or disabled.
Destination MAC Validation	Displays whether Destination MAC Validation is enabled or disabled.
IP Address Validation	Displays whether IP Address Validation is enabled or disabled.
VLAN	The VLAN ID for each displayed row.
Configuration	Displays whether DAI is enabled or disabled on the VLAN.
Log Invalid	Displays whether logging of invalid ARP packets is enabled on the VLAN.

Term	Definition
ACL Name	The ARP ACL Name, if configured on the VLAN.
Static Flag	If the ARP ACL is configured static on the VLAN.

The following shows example CLI display output for the command.

```
(CN1610) #show ip arp inspection vlan 10-12

Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled

 Vlan          Configuration    Log Invalid   ACL Name   Static flag
 ----          -------------    -----------   ---------  -----------
   10               Enabled        Enabled   H2          Enabled
   11              Disabled        Enabled
   12               Enabled       Disabled
```

show ip arp inspection statistics

Use this command to display the statistics of the ARP packets processed by Dynamic ARP Inspection. Give the vlan-list argument and the command displays the statistics on all DAI-enabled VLANs in that list. Give the single vlan argument and the command displays the statistics on that VLAN. If no argument is included, the command lists a summary of the forwarded and dropped ARP packets.

Format	`show ip arp inspection statistics [vlan vlan-list]`
Mode	◆ Privileged EXEC ◆ User EXEC

Term	Definition
VLAN	The VLAN ID for each displayed row.
Forwarded	The total number of valid ARP packets forwarded in this VLAN.
Dropped	The total number of not valid ARP packets dropped in this VLAN.

Term	Definition
DHCP Drops	The number of packets dropped due to DHCP snooping binding database match failure.
ACL Drops	The number of packets dropped due to ARP ACL rule match failure.
DHCP Permits	The number of packets permitted due to DHCP snooping binding database match.
ACL Permits	The number of packets permitted due to ARP ACL rule match.
Bad Src MAC	The number of packets dropped due to Source MAC validation failure.
Bad Dest MAC	The number of packets dropped due to Destination MAC validation failure.
Invalid IP	The number of packets dropped due to invalid IP checks.

The following shows example CLI display output for the command **show ip arp inspection statistics** which lists the summary of forwarded and dropped ARP packets on all DAI-enabled VLANs.

```
VLAN  Forwarded  Dropped
----  ---------  -------
  10         90       14
  20         10        3
```

The following shows example CLI display output for the command `show ip arp inspection statistics vlan` *`vlan-list`*.

```
VLAN    DHCP      ACL       DHCP       ACL       Bad Src   Bad Dest
Invalid
 Drops Drops      Permits    Permits      MAC       MAC        IP
----- -------- --------- ----------- --------- ---------- ---------
-- ---------
10  11 1  65         25 1 1         0
20  1 0 8          2 0 1         1
```

clear ip arp inspection statistics

Use this command to reset the statistics for Dynamic ARP Inspection on all VLANs.

Default	none
Format	clear ip arp inspection statistics
Mode	Privileged EXEC

show ip arp inspection interfaces

Use this command to display the Dynamic ARP Inspection configuration on all the DAI-enabled interfaces. An interface is said to be enabled for DAI if at least one VLAN, that the interface is a member of, is enabled for DAI. Given a slot/port interface argument, the command displays the values for that interface whether the interface is enabled for DAI or not.

Format	show ip arp inspection interfaces [slot/port]
Mode	◆ Privileged EXEC ◆ User EXEC

Term	Definition
Interface	The interface ID for each displayed row.
Trust State	Whether the interface is trusted or untrusted for DAI.
Rate Limit	The configured rate limit value in packets per second.
Burst Interval	The configured burst interval value in seconds.

The following shows example CLI display output for the command.

```
(CN1610) #show ip arp inspection interfaces

Interface    Trust State  Rate Limit  Burst Interval
                                 (pps)        (seconds)
--------------  -----------   ----------  ---------------
0/1               Untrusted          15               1
0/2               Untrusted          10              10
```

show arp access-list

Use this command to display the configured ARP ACLs with the rules. Giving an ARP ACL name as the argument will display only the rules in that ARP ACL.

Format	`show arp access-list [acl-name]`
Mode	◆ Privileged EXEC ◆ User EXEC

The following shows example CLI display output for the command.

```
(CN1610) #show arp access-list

ARP access list H2
    permit ip host 1.1.1.1 mac host 00:01:02:03:04:05
    permit ip host 1.1.1.2 mac host 00:03:04:05:06:07
ARP access list H3
ARP access list H4
    permit ip host 2.1.1.2 mac host 00:03:04:05:06:08
```

IGMP Snooping Configuration Commands

This section describes the commands you use to configure IGMP snooping. FASTPATH SMB software supports IGMP Versions 1, 2, and 3. The IGMP snooping feature can help conserve bandwidth because it allows the switch to forward IP multicast traffic only to connected hosts that request multicast traffic. IGMPv3 adds source filtering capabilities to IGMP versions 1 and 2.

Note

This note clarifies the prioritization of MGMD Snooping Configurations. Many of the IGMP/MLD Snooping commands are available both in the Interface and VLAN modes. Operationally the system chooses or prefers the VLAN configured values over the Interface configured values for most configurations when the interface participates in the VLAN.

set igmp

This command enables IGMP Snooping on the system (Global Config Mode), an interface, or a range of interfaces. This command also enables IGMP snooping on a particular VLAN (VLAN Config Mode) and can enable IGMP snooping on all interfaces participating in a VLAN.

If an interface has IGMP Snooping enabled and you enable this interface for routing or enlist it as a member of a port-channel (LAG), IGMP Snooping functionality is disabled on that interface. IGMP Snooping functionality is re-enabled if you disable routing or remove port-channel (LAG) membership from an interface that has IGMP Snooping enabled.

The IGMP application supports the following activities:

- Validation of the IP header checksum (as well as the IGMP header checksum) and discarding of the frame upon checksum error.
- Maintenance of the forwarding table entries based on the MAC address versus the IP address.
- Flooding of unregistered multicast data packets to all ports in the VLAN.

Default	disabled
Format	`set igmp [vlan_id]`
Mode	◆ Global Config ◆ Interface Config ◆ VLAN Config

no set igmp

This command disables IGMP Snooping on the system, an interface, a range of interfaces, or a VLAN.

Format	`no set igmp [vlan_id]`
Mode	◆ Global Config ◆ Interface Config ◆ VLAN Config

set igmp header-validation

This command enables header validation for IGMP messages.

When header validation is enabled, IGMP Snooping checks:

- The time-to-live(TTL) field in the IGMP header and drops packets where TTL is not equal to 1. The TTL field should always be set to 1 in the headers of IGMP reports and queries.
- The presence of the router alert option (9404) in the IP packet header of the IGMPv2 message and drops packets that do not include this option.
- The presence of the router alert option (9404) and ToS Byte = 0xC0 (Internet Control) in the IP packet header of IGMPv3 message and drops packets that do not include these options.

Default	enabled
Format	`set igmp header-validation`
Mode	Global Config

no set igmp header-validation

This command disables header validation for IGMP messages.

Format	`no set igmp header-validation`
Mode	Global Config

set igmp interfacemode

This command enables IGMP Snooping on all interfaces. If an interface has IGMP Snooping enabled and you enable this interface for routing or enlist it as a member of a port-channel (LAG), IGMP Snooping functionality is disabled on

that interface. IGMP Snooping functionality is re-enabled if you disable routing or remove port-channel (LAG) membership from an interface that has IGMP Snooping enabled.

Default	disabled
Format	`set igmp interfacemode`
Mode	Global Config

no set igmp interfacemode

This command disables IGMP Snooping on all interfaces.

Format	`no set igmp interfacemode`
Mode	Global Config

set igmp fast-leave

This command enables or disables IGMP Snooping fast-leave admin mode on a selected interface, a range of interfaces, or a VLAN. Enabling fast-leave allows the switch to immediately remove the layer 2 LAN interface from its forwarding table entry upon receiving an IGMP leave message for that multicast group without first sending out MAC-based general queries to the interface.

You should enable fast-leave admin mode only on VLANs where only one host is connected to each layer 2 LAN port. This prevents the inadvertent dropping of the other hosts that were connected to the same layer 2 LAN port but were still interested in receiving multicast traffic directed to that group. Also, fast-leave processing is supported only with IGMP version 2 hosts.

Default	disabled
Format	`set igmp fast-leave [`*`vlan_id`*`]`
Mode	Interface Config Interface Range VLAN Config

no set igmp fast-leave

This command disables IGMP Snooping fast-leave admin mode on a selected interface.

Format	`no set igmp fast-leave [vlan_id]`
Mode	Interface Config Interface Range VLAN Config

set igmp groupmembership-interval

This command sets the IGMP Group Membership Interval time on a VLAN, one interface, a range of interfaces, or all interfaces. The Group Membership Interval time is the amount of time in seconds that a switch waits for a report from a particular group on a particular interface before deleting the interface from the entry. This value must be greater than the IGMPv3 Maximum Response time value. The range is 2 to 3600 seconds.

Default	260 seconds
Format	`set igmp groupmembership-interval [vlan_id] 2-3600`
Mode	◆ Interface Config ◆ Global Config ◆ VLAN Config

no set igmp groupmembership-interval

This command sets the IGMPv3 Group Membership Interval time to the default value.

Format	`no set igmp groupmembership-interval [vlan_id]`
Mode	◆ Interface Config ◆ Global Config ◆ VLAN Config

set igmp maxresponse

This command sets the IGMP Maximum Response time for the system, on a particular interface or VLAN, or on a range of interfaces. The Maximum Response time is the amount of time in seconds that a switch will wait after

sending a query on an interface because it did not receive a report for a particular group in that interface. This value must be less than the IGMP Query Interval time value. The range is 1 to 25 seconds.

Default	10 seconds
Format	`set igmp maxresponse [vlan_id] 1-25`
Mode	◆ Global Config ◆ Interface Config ◆ VLAN Config

no set igmp maxresponse

This command sets the max response time (on the interface or VLAN) to the default value.

Format	`no set igmp maxresponse [vlan_id]`
Mode	◆ Global Config ◆ Interface Config ◆ VLAN Config

set igmp mcrtrexpiretime

This command sets the Multicast Router Present Expiration time. The time is set for the system, on a particular interface or VLAN, or on a range of interfaces. This is the amount of time in seconds that a switch waits for a query to be received on an interface before the interface is removed from the list of interfaces with multicast routers attached. The range is 0 to 3600 seconds. A value of 0 indicates an infinite time-out, i.e. no expiration.

Default	0
Format	`set igmp mcrtrexpiretime [vlan_id] 0-3600`
Mode	◆ Global Config ◆ Interface Config ◆ VLAN Config

no set igmp mcrtrexpiretime

This command sets the Multicast Router Present Expiration time to 0. The time is set for the system, on a particular interface or a VLAN.

Format	`no set igmp mcrtrexpiretime [vlan_id]`
Mode	◆ Global Config ◆ Interface Config ◆ VLAN Config

Format	`no set igmp mcrtrexpiretime vlan_id`
Mode	VLAN Config

set igmp mrouter

This command configures the VLAN ID (*vlan_id*) that has the multicast router mode enabled.

Format	`set igmp mrouter vlan_id`
Mode	Interface Config

no set igmp mrouter

This command disables multicast router mode for a particular VLAN ID (*vlan_id*).

Format	`no set igmp mrouter vlan_id`
Mode	Interface Config

set igmp mrouter interface

This command configures the interface or range of interfaces as a multicast router interface. When configured as a multicast router interface, the interface is treated as a multicast router interface in all VLANs.

Default	disabled
Format	`set igmp mrouter interface`
Mode	Interface Config

no set igmp mrouter interface

This command disables the status of the interface as a statically configured multicast router interface.

Format	`no set igmp mrouter interface`
Mode	Interface Config

set igmp report-suppression

Use this command to suppress the IGMP reports on a given VLAN ID. In order to optimize the number of reports traversing the network with no added benefits, a Report Suppression mechanism is implemented. When more than one client responds to an MGMD query for the same Multicast Group address within the max-response-time, only the first response is forwarded to the query and others are suppressed at the switch.

Default	Disabled
Format	`set igmp report-suppression` *`vlan-id`*
Mode	VLAN Config

Parameter	Description
vlan-id	A valid VLAN ID. Range is 1 to 4093.

The following shows an example of the command.

```
(Broadcom FASTPATH Switching) #vlan database
(Broadcom FASTPATH Switching) (Vlan)#set igmp report-suppression ?

<1-4093>                  Enter VLAN ID.

(Broadcom FASTPATH Switching) (Vlan)#set igmp report-suppression 1
```

no set igmp report-suppression

Use this command to return the system to the default.

Format	`no set igmp report-suppression`
Mode	VLAN Config

show igmpsnooping

This command displays IGMP Snooping information for a given slot/port or VLAN. Configured information is displayed whether or not IGMP Snooping is enabled.

Format	`show igmpsnooping [slot/port | vlan_id]`
Mode	Privileged EXEC

When the optional arguments slot/port or *vlan_id* are not used, the command displays the following information:

Term	Definition
Admin Mode	Indicates whether or not IGMP Snooping is active on the switch.
Multicast Control Frame Count	The number of multicast control frames that are processed by the CPU.
Interface Enabled for IGMP Snooping	The list of interfaces on which IGMP Snooping is enabled.
VLANS Enabled for IGMP Snooping	The list of VLANS on which IGMP Snooping is enabled.

When you specify the slot/port values, the following information appears:

Term	Definition
IGMP Snooping Admin Mode	Indicates whether IGMP Snooping is active on the interface.
Fast Leave Mode	Indicates whether IGMP Snooping Fast-leave is active on the interface.
Group Membership Interval	The amount of time in seconds that a switch will wait for a report from a particular group on a particular interface before deleting the interface from the entry.This value may be configured.

Term	Definition
Maximum Response Time	The amount of time the switch waits after it sends a query on an interface because it did not receive a report for a particular group on that interface. This value may be configured.
Multicast Router Expiry Time	The amount of time to wait before removing an interface from the list of interfaces with multicast routers attached. The interface is removed if a query is not received. This value may be configured.

When you specify a value for *vlan_id*, the following information appears:

Term	Definition
VLAN ID	The VLAN ID.
IGMP Snooping Admin Mode	Indicates whether IGMP Snooping is active on the VLAN.
Fast Leave Mode	Indicates whether IGMP Snooping Fast-leave is active on the VLAN.
Group Membership Interval (secs)	The amount of time in seconds that a switch will wait for a report from a particular group on a particular interface, which is participating in the VLAN, before deleting the interface from the entry.This value may be configured.
Maximum Response Time (secs)	The amount of time the switch waits after it sends a query on an interface, participating in the VLAN, because it did not receive a report for a particular group on that interface. This value may be configured.
Multicast Router Expiry Time (secs)	The amount of time to wait before removing an interface that is participating in the VLAN from the list of interfaces with multicast routers attached. The interface is removed if a query is not received. This value may be configured.

Term	Definition
Report Suppression Mode	Indicates whether IGMP reports (set by the command "set igmp report-suppression" on page 514) in enabled or not.

The following shows example CLI display output for the command.

```
(Broadcom FASTPATH Switching) #show igmpsnooping 1

VLAN ID..................................... 1
IGMP Snooping Admin Mode.................... Disabled
Fast Leave Mode............................. Disabled
Group Membership Interval (secs)............ 260
Max Response Time (secs).................... 10
Multicast Router Expiry Time (secs)......... 0
Report Suppression Mode..................... Enabled
```

show igmpsnooping mrouter vlan

This command displays information about statically configured ports.

Format	`show igmpsnooping mrouter vlan slot/port`
Mode	Privileged EXEC

Term	Definition
Interface	The port on which multicast router information is being displayed.
VLAN ID	The list of VLANs of which the interface is a member.

show igmpsnooping ssm

This command displays information about Source Specific Multicasting (SSM) by entry, group, or statistics. SSM delivers multicast packets to receivers that originated from a source address specified by the receiver. SSM is only available with IGMPv3 and MLDv2.

Format	`show igmpsnooping ssm {entries | groups | stats}`

Mode	Privileged EXEC

show mac-address-table igmpsnooping

This command displays the IGMP Snooping entries in the MFDB table.

Format	`show mac-address-table igmpsnooping`
Mode	Privileged EXEC

Term	Definition
VLAN ID	The VLAN in which the MAC address is learned.
MAC Address	A multicast MAC address for which the switch has forwarding or filtering information. The format is 6 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB.
Type	The type of the entry, which is either static (added by the user) or dynamic (added to the table as a result of a learning process or protocol).
Description	The text description of this multicast table entry.
Interfaces	The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).

IGMP Snooping Querier Commands

IGMP Snooping requires that one central switch or router periodically query all end-devices on the network to announce their multicast memberships. This central device is the “IGMP Querier”. The IGMP query responses, known as IGMP reports, keep the switch updated with the current multicast group membership on a port-by-port basis. If the switch does not receive updated membership information in a timely fashion, it will stop forwarding multicasts to the port where the end device is located.

This section describes commands used to configure and display information on IGMP Snooping Queriers on the network and, separately, on VLANs.

Note
This note clarifies the prioritization of MGMD Snooping Configurations. Many of the IGMP/MLD Snooping commands are available both in the Interface and VLAN modes. Operationally the system chooses or prefers the VLAN configured values over the Interface configured values for most configurations when the interface participates in the VLAN.

set igmp querier

Use this command to enable IGMP Snooping Querier on the system, using Global Config mode, or on a VLAN. Using this command, you can specify the IP Address that the Snooping Querier switch should use as the source address while generating periodic queries.

If a VLAN has IGMP Snooping Querier enabled and IGMP Snooping is operationally disabled on it, IGMP Snooping Querier functionality is disabled on that VLAN. IGMP Snooping functionality is re-enabled if IGMP Snooping is operational on the VLAN.

Note
The Querier IP Address assigned for a VLAN takes preference over global configuration.

The IGMP Snooping Querier application supports sending periodic general queries on the VLAN to solicit membership reports.

Default	disabled
Format	`set igmp querier [`*`vlan-id`*`] [address `*`ipv4_address`*`]`

Mode	◆ Global Config ◆ VLAN Mode

no set igmp querier

Use this command to disable IGMP Snooping Querier on the system. Use the optional `address` parameter to reset the querier address to 0.0.0.0.

Format	`no set igmp querier [vlan-id] [address]`
Mode	◆ Global Config ◆ VLAN Mode

set igmp querier query-interval

Use this command to set the IGMP Querier Query Interval time. It is the amount of time in seconds that the switch waits before sending another general query.

Default	disabled
Format	`set igmp querier query-interval 1-1800`
Mode	Global Config

no set igmp querier query-interval

Use this command to set the IGMP Querier Query Interval time to its default value.

Format	`no set igmp querier query-interval`
Mode	Global Config

set igmp querier timer expiry

Use this command to set the IGMP Querier timer expiration period. It is the time period that the switch remains in Non-Querier mode once it has discovered that there is a Multicast Querier in the network.

Default	60 seconds
Format	`set igmp querier timer expiry 60-300`
Mode	Global Config

no set igmp querier timer expiry

Use this command to set the IGMP Querier timer expiration period to its default value.

Format	`no set igmp querier timer expiry`
Mode	Global Config

set igmp querier version

Use this command to set the IGMP version of the query that the snooping switch is going to send periodically.

Default	1
Format	`set igmp querier version` *1-2*
Mode	Global Config

no set igmp querier version

Use this command to set the IGMP Querier version to its default value.

Format	`no set igmp querier version`
Mode	Global Config

set igmp querier election participate

Use this command to enable the Snooping Querier to participate in the Querier Election process when it discovers the presence of another Querier in the VLAN. When this mode is enabled, if the Snooping Querier finds that the other Querier's source address is better (less) than the Snooping Querier's address, it stops sending periodic queries. If the Snooping Querier wins the election, then it will continue sending periodic queries.

Default	disabled
Format	`set igmp querier election participate`
Mode	VLAN Config

no set igmp querier election participate

Use this command to set the Snooping Querier not to participate in querier election but go into non-querier mode as soon as it discovers the presence of another querier in the same VLAN.

Format	`no set igmp querier election participate`
Mode	VLAN Config

show igmpsnooping querier

Use this command to display IGMP Snooping Querier information. Configured information is displayed whether or not IGMP Snooping Querier is enabled.

Format	`show igmpsnooping querier [{detail | vlan` *`vlanid`*`}]`
Mode	Privileged EXEC

When the optional argument *`vlanid`* is not used, the command displays the following information.

Field	Description
Admin Mode	Indicates whether or not IGMP Snooping Querier is active on the switch.
Admin Version	The version of IGMP that will be used while sending out the queries.
Querier Address	The IP Address which will be used in the IPv4 header while sending out IGMP queries. It can be configured using the appropriate command.
Query Interval	The amount of time in seconds that a Snooping Querier waits before sending out the periodic general query.
Querier Timeout	The amount of time to wait in the Non-Querier operational state before moving to a Querier state.

When you specify a value for *vlanid*, the following additional information appears.

Field	Description
VLAN Admin Mode	Indicates whether iGMP Snooping Querier is active on the VLAN.
VLAN Operational State	Indicates whether IGMP Snooping Querier is in "Querier" or "Non-Querier" state. When the switch is in *Querier* state, it will send out periodic general queries. When in *Non-Querier* state, it will wait for moving to Querier state and does not send out any queries.
VLAN Operational Max Response Time	Indicates the time to wait before removing a Leave from a host upon receiving a Leave request. This value is calculated dynamically from the Queries received from the network. If the Snooping Switch is in Querier state, then it is equal to the configured value.
Querier Election Participation	Indicates whether the IGMP Snooping Querier participates in querier election if it discovers the presence of a querier in the VLAN.
Querier VLAN Address	The IP address will be used in the IPv4 header while sending out IGMP queries on this VLAN. It can be configured using the appropriate command.
Operational Version	The version of IPv4 will be used while sending out IGMP queries on this VLAN.
Last Querier Address	Indicates the IP address of the most recent Querier from which a Query was received.
Last Querier Version	Indicates the IGMP version of the most recent Querier from which a Query was received on this VLAN.

When the optional argument `detail` is used, the command shows the global information and the information for all Querier-enabled VLANs.

MLD Snooping Commands

This section describes commands used for MLD Snooping. In IPv4, Layer 2 switches can use IGMP Snooping to limit the flooding of multicast traffic by dynamically configuring Layer 2 interfaces so that multicast traffic is forwarded only to those interfaces associated with IP multicast addresses. In IPv6, MLD Snooping performs a similar function. With MLD Snooping, IPv6 multicast data is selectively forwarded to a list of ports that want to receive the data, instead of being flooded to all ports in a VLAN. This list is constructed by snooping IPv6 multicast control packets.

Note

This note clarifies the prioritization of MGMD Snooping Configurations. Many of the IGMP/MLD Snooping commands are available both in the Interface and VLAN modes. Operationally the system chooses or prefers the VLAN configured values over the Interface configured values for most configurations when the interface participates in the VLAN.

set mld

This command enables MLD Snooping on the system (Global Config Mode) or an Interface (Interface Config Mode). This command also enables MLD Snooping on a particular VLAN and enables MLD Snooping on all interfaces participating in a VLAN.

If an interface has MLD Snooping enabled and you enable this interface for routing or enlist it as a member of a port-channel (LAG), MLD Snooping functionality is disabled on that interface. MLD Snooping functionality is re-enabled if you disable routing or remove port channel (LAG) membership from an interface that has MLD Snooping enabled.

MLD Snooping supports the following activities:

- Validation of address version, payload length consistencies and discarding of the frame upon error.
- Maintenance of the forwarding table entries based on the MAC address versus the IPv6 address.
- Flooding of unregistered multicast data packets to all ports in the VLAN.

Default	disabled
Format	`set mld` *`vlanid`*

Mode	◆ Global Config ◆ Interface Config ◆ VLAN Mode

no set mld

Use this command to disable MLD Snooping on the system.

Format	`set mld` *`vlanid`*
Mode	◆ Global Config ◆ Interface Config ◆ VLAN Mode

set mld interfacemode

Use this command to enable MLD Snooping on all interfaces. If an interface has MLD Snooping enabled and you enable this interface for routing or enlist it as a member of a port-channel (LAG), MLD Snooping functionality is disabled on that interface. MLD Snooping functionality is re-enabled if you disable routing or remove port-channel (LAG) membership from an interface that has MLD Snooping enabled.

Default	disabled
Format	`set mld interfacemode`
Mode	Global Config

no set mld interfacemode

Use this command to disable MLD Snooping on all interfaces.

Format	`no set mld interfacemode`
Mode	Global Config

set mld fast-leave

Use this command to enable MLD Snooping fast-leave admin mode on a selected interface or VLAN. Enabling fast-leave allows the switch to immediately remove the Layer 2 LAN interface from its forwarding table entry upon receiving and MLD done message for that multicast group without first sending out MAC-based general queries to the interface.

Note
You should enable fast-leave admin mode only on VLANs where only one host is connected to each Layer 2 LAN port. This prevents the inadvertent dropping of the other hosts that were connected to the same layer 2 LAN port but were still interested in receiving multicast traffic directed to that group.

Note
Fast-leave processing is supported only with MLD version 1 hosts.

Default	disabled
Format	`set mld fast-leave` *`vlanid`*
Mode	◆ Interface Config ◆ VLAN Mode

no set mld fast-leave

Use this command to disable MLD Snooping fast-leave admin mode on a selected interface.

Format	`no set mld fast-leave` *`vlanid`*
Mode	◆ Interface Config ◆ VLAN Mode

set mld groupmembership-interval

Use this command to set the MLD Group Membership Interval time on a VLAN, one interface or all interfaces. The Group Membership Interval time is the amount of time in seconds that a switch waits for a report from a particular group on a particular interface before deleting the interface from the entry. This value must be greater than the MLDv2 Maximum Response time value. The range is 2 to 3600 seconds.

Default	260 seconds

Format	`set mld groupmembership-interval` *`vlanid 2-3600`*
Mode	◆ Interface Config ◆ Global Config ◆ VLAN Mode

no set groupmembership-interval

Use this command to set the MLDv2 Group Membership Interval time to the default value.

Format	`no set mld groupmembership-interval`
Mode	◆ Interface Config ◆ Global Config ◆ VLAN Mode

set mld maxresponse

Use this command to set the MLD Maximum Response time for the system, on a particular interface or VLAN. The Maximum Response time is the amount of time in seconds that a switch will wait after sending a query on an interface because it did not receive a report for a particular group in that interface. This value must be less than the MLD Query Interval time value. The range is 1 to 65 seconds.

Default	10 seconds
Format	`set mld maxresponse` *`1-65`*
Mode	◆ Global Config ◆ Interface Config ◆ VLAN Mode

no set mld maxresponse

Use this command to set the max response time (on the interface or VLAN) to the default value.

Format	`no set mld maxresponse`

Mode	◆ Global Config ◆ Interface Config ◆ VLAN Mode

set mld mcrtexpiretime

Use this command to set the Multicast Router Present Expiration time. The time is set for the system, on a particular interface or VLAN. This is the amount of time in seconds that a switch waits for a query to be received on an interface before the interface is removed from the list of interfaces with multicast routers attached. The range is 0 to 3600 seconds. A value of 0 indicates an infinite timeout, i.e. no expiration.

Default	0
Format	`set mld mcrtexpiretime` *`vlanid 0-3600`*
Mode	◆ Global Config ◆ Interface Config

no set mld mcrtexpiretime

Use this command to set the Multicast Router Present Expiration time to 0. The time is set for the system, on a particular interface or a VLAN.

Format	`no set mld mcrtexpiretime` *`vlanid`*
Mode	◆ Global Config ◆ Interface Config

set mld mrouter

Use this command to configure the VLAN ID for the VLAN that has the multicast router attached mode enabled.

Format	`set mld mrouter` *`vlanid`*
Mode	Interface Config

no set mld mrouter

Use this command to disable multicast router attached mode for a VLAN with a particular VLAN ID.

Format	`no set mld mrouter vlanid`
Mode	Interface Config

set mld mrouter interface

Use this command to configure the interface as a multicast router-attached interface. When configured as a multicast router interface, the interface is treated as a multicast router-attached interface in all VLANs.

Default	disabled
Format	`set mld mrouter interface`
Mode	Interface Config

no set mld mrouter interface

Use this command to disable the status of the interface as a statically configured multicast router-attached interface.

Format	`no set mld mrouter interface`
Mode	Interface Config

show mldsnooping

Use this command to display MLD Snooping information. Configured information is displayed whether or not MLD Snooping is enabled.

Format	`show mldsnooping [unit/slot/port | vlanid]`
Mode	Privileged EXEC

When the optional arguments *unit/slot/port* or *vlanid* are not used, the command displays the following information.

Term	Definition
Admin Mode	Indicates whether or not MLD Snooping is active on the switch.

Term	Definition
Interfaces Enabled for MLD Snooping	Interfaces on which MLD Snooping is enabled.
MLD Control Frame Count	Displays the number of MLD Control frames that are processed by the CPU.
VLANs Enabled for MLD Snooping	VLANs on which MLD Snooping is enabled.

When you specify the *unit/slot/port* values, the following information displays.

Term	Definition
MLD Snooping Admin Mode	Indicates whether MLD Snooping is active on the interface.
Fast Leave Mode	Indicates whether MLD Snooping Fast Leave is active on the VLAN.
Group Membership Interval	Shows the amount of time in seconds that a switch will wait for a report from a particular group on a particular interface, which is participating in the VLAN, before deleting the interface from the entry. This value may be configured.
Max Response Time	Displays the amount of time the switch waits after it sends a query on an interface, participating in the VLAN, because it did not receive a report for a particular group on that interface. This value may be configured.
Multicast Router Present Expiration Time	Displays the amount of time to wait before removing an interface that is participating in the VLAN from the list of interfaces with multicast routers attached. The interface is removed if a query is not received. This value may be configured.

When you specify a value for *vlanid*, the following information appears.

Term	Definition
VLAN Admin Mode	Indicates whether MLD Snooping is active on the VLAN.

show mldsnooping mrouter interface

Use this command to display information about statically configured multicast router attached interfaces.

Format	`show mldsnooping mrouter interface` *`unit/slot/port`*
Mode	Privileged EXEC

Term	Definition
Interface	Shows the interface on which multicast router information is being displayed.
Multicast Router Attached	Indicates whether multicast router is statically enabled on the interface.

show mldsnooping mrouter vlan

Use this command to display information about statically configured multicast router-attached interfaces.

Format	`show mldsnooping mrouter vlan` *`unit/slot/port`*
Mode	Privileged EXEC

Term	Definition
Interface	Shows the interface on which multicast router information is being displayed.
VLAN ID	Displays the list of VLANs of which the interface is a member.

show mldsnooping ssm entries

Use this command to display the source specific multicast forwarding database built by MLD snooping.

A given {Source, Group, VLAN} combination can have few interfaces in INCLUDE mode and few interfaces in EXCLUDE mode. In such instances, two rows for the same {Source, Group, VLAN} combinations are displayed.

Format	`show mldsnooping ssm entries`
Mode	Privileged EXEC

Term	**Definition**
VLAN	The VLAN on which the entry is learned.
Group	The IPv6 multicast group address.
Source	The IPv6 source address.
Source Filter Mode	The source filter mode (Include/Exclude) for the specified group.
Interfaces	1)If Source Filter Mode is “Include,” specifies the list of interfaces on which a incoming packet is forwarded. If it’s source IP address is equal to the current entry’s Source, the destination IP address is equal to the current entry’s Group and the VLAN ID on which it arrived is current entry’s VLAN. 2) If Source Filter Mode is “Exclude,” specifies the list of interfaces on which a incoming packet is forwarded. If it’s source IP address is *not* equal to the current entry’s Source, the destination IP address is equal to current entry’s Group and VLAN ID on which it arrived is current entry’s VLAN.

show mldsnooping ssm stats

Use this command to display the statistics of MLD snooping’s SSMFDB. This command takes no options.

Format	`show mldsnooping ssm stats`

Mode	Privileged EXEC

Term	Definition
Total Entries	The total number of entries that can possibly be in the MLD snooping's SSMFDB.
Most SSMFDB Entries Ever Used	The largest number of entries that have been present in the MLD snooping's SSMFDB.
Current Entries	The current number of entries in the MLD snooping's SSMFDB.

show mldsnooping ssm groups

Use this command to display the MLD SSM group membership information.

Format	`show mldsnooping ssm groups`
Mode	Privileged EXEC

Term	Definition
VLAN	VLAN on which the MLD v2 report is received.
Group	The IPv6 multicast group address.
Interface	The interface on which the MLD v2 report is received.
Reporter	The IPv6 address of the host that sent the MLDv2 report.
Source Filter Mode	The source filter mode (Include/Exclude) for the specified group.
Source Address List	List of source IP addresses for which source filtering is requested.

show mac-address-table mldsnooping

Use this command to display the MLD Snooping entries in the Multicast Forwarding Database (MFDB) table.

Format	`show mac-address-table mldsnooping`
Mode	Privileged EXEC

Term	Definition
VLAN ID	The VLAN in which the MAC address is learned.
MAC Address	A multicast MAC address for which the switch has forwarding or filtering information. The format is 6 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB.
Type	The type of entry, which is either static (added by the user) or dynamic (added to the table as a result of a learning process or protocol.)
Description	The text description of this multicast table entry.
Interfaces	The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).

clear mldsnooping

Use this command to delete all MLD snooping entries from the MFDB table.

Format	`clear mldsnooping`
Mode	Privileged EXEC

MLD Snooping Querier Commands

In an IPv6 environment, MLD Snooping requires that one central switch or router periodically query all end-devices on the network to announce their multicast memberships. This central device is the MLD Querier. The MLD query responses, known as MLD reports, keep the switch updated with the current multicast group membership on a port-by-port basis. If the switch does not receive updated membership information in a timely fashion, it will stop forwarding multicasts to the port where the end device is located.

This section describes the commands you use to configure and display information on MLD Snooping queries on the network and, separately, on VLANs.

Note

This note clarifies the prioritization of MGMD Snooping Configurations. Many of the IGMP/MLD Snooping commands are available both in the Interface and VLAN modes. Operationally the system chooses or prefers the VLAN configured values over the Interface configured values for most configurations when the interface participates in the VLAN.

set mld querier

Use this command to enable MLD Snooping Querier on the system (Global Config Mode) or on a VLAN. Using this command, you can specify the IP address that the snooping querier switch should use as a source address while generating periodic queries.

If a VLAN has MLD Snooping Querier enabled and MLD Snooping is operationally disabled on it, MLD Snooping Querier functionality is disabled on that VLAN. MLD Snooping functionality is re-enabled if MLD Snooping is operational on the VLAN.

The MLD Snooping Querier sends periodic general queries on the VLAN to solicit membership reports.

Default	disabled
Format	`set mld querier` *`[vlan-id]`* `[address` *`ipv6_address]`*
Mode	◆ Global Config ◆ VLAN Mode

no set mld querier

Use this command to disable MLD Snooping Querier on the system. Use the optional parameter `address` to reset the querier address.

Format	`no set mld querier [vlan-id][address]`
Mode	◆ Global Config ◆ VLAN Mode

set mld querier query_interval

Use this command to set the MLD Querier Query Interval time. It is the amount of time in seconds that the switch waits before sending another general query.

Default	60 seconds
Format	`set mld querier query_interval 1-1800`
Mode	Global Config

no set mld querier query_interval

Use this command to set the MLD Querier Query Interval time to its default value.

Format	`no set mld querier query_interval`
Mode	Global Config

set mld querier timer expiry

Use this command to set the MLD Querier timer expiration period. It is the time period that the switch remains in Non-Querier mode once it has discovered that there is a Multicast Querier in the network.

Default	60 seconds
Format	`set mld querier timer expiry 60-300`
Mode	Global Config

no set mld querier timer expiry

Use this command to set the MLD Querier timer expiration period to its default value.

Format	`no set mld querier timer expiry`
Mode	Global Config

set mld querier election participate

Use this command to enable the Snooping Querier to participate in the Querier Election process when it discovers the presence of another Querier in the VLAN. When this mode is enabled, if the Snooping Querier finds that the other Querier's source address is better (less) than the Snooping Querier's address, it stops sending periodic queries. If the Snooping Querier wins the election, then it will continue sending periodic queries.

Default	disabled
Format	`set mld querier election participate`
Mode	VLAN Config

no set mld querier election participate

Use this command to set the snooping querier not to participate in querier election but go into a non-querier mode as soon as it discovers the presence of another querier in the same VLAN.

Format	`no set mld querier election participate`
Mode	VLAN Config

show mldsnooping querier

Use this command to display MLD Snooping Querier information. Configured information is displayed whether or not MLD Snooping Querier is enabled.

Format	`show mldsnooping querier [{detail | vlan` *`vlanid`*`}]`
Mode	Privileged EXEC

When the optional arguments *`vlandid`* are not used, the command displays the following information.

Field	Description
Admin Mode	Indicates whether or not MLD Snooping Querier is active on the switch.
Admin Version	Indicates the version of MLD that will be used while sending out the queries. This is defaulted to MLD v1 and it cannot be changed.
Querier Address	Shows the IP address which will be used in the IPv6 header while sending out MLD queries. It can be configured using the appropriate command.
Query Interval	Shows the amount of time in seconds that a Snooping Querier waits before sending out the periodic general query.
Querier Timeout	Displays the amount of time to wait in the Non-Querier operational state before moving to a Querier state.

When you specify a value for *vlanid*, the following information appears.

Field	Description
VLAN Admin Mode	Indicates whether MLD Snooping Querier is active on the VLAN.
VLAN Operational State	Indicates whether MLD Snooping Querier is in "*Querier*" or "*Non-Querier*" state. When the switch is in *Querier* state, it will send out periodic general queries. When in *Non-Querier* state, it will wait for moving to *Querier* state and does not send out any queries.
VLAN Operational Max Response Time	Indicates the time to wait before removing a Leave from a host upon receiving a Leave request. This value is calculated dynamically from the Queries received from the network. If the Snooping Switch is in Querier state, then it is equal to the configured value.

Field	Description
Querier Election Participate	Indicates whether the MLD Snooping Querier participates in querier election if it discovers the presence of a querier in the VLAN.
Querier VLAN Address	The IP address will be used in the IPv6 header while sending out MLD queries on this VLAN. It can be configured using the appropriate command.
Operational Version	This version of IPv6 will be used while sending out MLD queriers on this VLAN.
Last Querier Address	Indicates the IP address of the most recent Querier from which a Query was received.
Last Querier Version	Indicates the MLD version of the most recent Querier from which a Query was received on this VLAN.

When the optional argument `detail` is used, the command shows the global information and the information for all Querier-enabled VLANs.

Port Security Commands

This section describes the command you use to configure Port Security on the switch. Port security, which is also known as port MAC locking, allows you to secure the network by locking allowable MAC addresses on a given port. Packets with a matching source MAC address are forwarded normally, and all other packets are discarded.

Note

To enable the SNMP trap specific to port security, see "snmp-server enable traps violation" on page 91.

port-security

This command enables port locking on an interface, a range of interfaces, or at the system level.

Default	disabled
Format	`port-security`
Mode	◆ Global Config (to enable port locking globally) ◆ Interface Config (to enable port locking on an interface or range of interfaces)

no port-security

This command disables port locking for one (Interface Config) or all (Global Config) ports.

Format	`no port-security`
Mode	◆ Global Config ◆ Interface Config

port-security max-dynamic

This command sets the maximum number of dynamically locked MAC addresses allowed on a specific port. The valid range is 0–600.

Default	600
Format	`port-security max-dynamic` *`maxvalue`*

Mode	Interface Config

no port-security max-dynamic

This command resets the maximum number of dynamically locked MAC addresses allowed on a specific port to its default value.

Format	`no port-security max-dynamic`
Mode	Interface Config

port-security max-static

This command sets the maximum number of statically locked MAC addresses allowed on a port. The valid range is 0–20.

Default	1
Format	`port-security max-static` *`maxvalue`*
Mode	Interface Config

no port-security max-static

This command sets maximum number of statically locked MAC addresses to the default value.

Format	`no port-security max-static`
Mode	Interface Config

port-security mac-address

This command adds a MAC address to the list of statically locked MAC addresses for an interface or range of interfaces. The *`vid`* is the VLAN ID.

Format	`port-security mac-address` *`mac-address vid`*
Mode	Interface Config

no port-security mac-address

This command removes a MAC address from the list of statically locked MAC addresses.

Format	`no port-security mac-address` *`mac-address vid`*
Mode	Interface Config

port-security mac-address move

This command converts dynamically locked MAC addresses to statically locked addresses for an interface or range of interfaces.

Format	`port-security mac-address move`
Mode	Interface Config

port-security mac-address sticky

This command enables sticky mode Port MAC Locking on a port. If accompanied by a MAC address and a VLAN id (for interface config mode only), it adds a sticky MAC address to the list of statically locked MAC addresses. These sticky addresses are converted back to dynamically locked addresses if sticky mode is disabled on the port. The <vid> is the VLAN ID. The Global command applies the "sticky" mode to all valid interfaces (physical and LAG). There is no global sticky mode as such.

Sticky addresses that are dynamically learned will appear in "show running-config" on page 177 as "port-security mac-address sticky <mac> <vid>" entries. This distinguishes them from static entries.

Format	`port-security mac-address sticky [<mac-address> <vid>]`
Mode	◆ Global Config ◆ Interface Config

The following shows an example of the command.

```
(CN1610)(Config)# port-security mac-address sticky
(CN1610)(Interface)# port-security mac-address sticky
(CN1610)(Interface)# port-security mac-address sticky
  00:00:00:00:00:01 2
```

no port-security mac-address sticky

The **no** form removes the sticky mode. The sticky MAC address can be deleted by using the command "no port-security mac-address <mac-address> <vid>".

Format	`no port-security mac-address sticky [<mac-address> <vid>]`
Mode	◆ Global Config ◆ Interface Config

show port-security

This command displays the port-security settings for the port(s). If you do not use a parameter, the command displays the Port Security Administrative mode. Use the optional parameters to display the settings on a specific interface or on all interfaces. Instead of slot/port, `lag` *`lag-intf-num`* can be used as an alternate way to specify the LAG interface. `lag` *`lag-intf-num`* can also be used to specify the LAG interface where *`lag-intf-num`* is the LAG port number.

Format	`show port-security [{slot/port | all}]`
Mode	Privileged EXEC

Term	Definition
Admin Mode	Port Locking mode for the entire system. This field displays if you do not supply any parameters.

For each interface, or for the interface you specify, the following information appears:

Term	Definition
Admin Mode	Port Locking mode for the Interface.
Dynamic Limit	Maximum dynamically allocated MAC Addresses.
Static Limit	Maximum statically allocated MAC Addresses.
Violation Trap Mode	Whether violation traps are enabled.
Sticky Mode	The administrative mode of the port security Sticky Mode feature on the interface.

The following shows example CLI display output for the command.

```
(CN1610) #show port-security 0/1
```

```
        Admin    Dynamic     Static     Violation  Sticky
Intf    Mode      Limit      Limit      Trap Mode  Mode
------  -------  ----------  ---------  ---------  --------
0/1     Disabled 1           1          Disabled   Enabled
```

show port-security dynamic

This command displays the dynamically locked MAC addresses for the port. Instead of slot/port, `lag` *`lag-intf-num`* can be used as an alternate way to specify the LAG interface. `lag` *`lag-intf-num`* can also be used to specify the LAG interface where *`lag-intf-num`* is the LAG port number.

Format	`show port-security dynamic` slot/port
Mode	Privileged EXEC

Term	Definition
MAC Address	MAC Address of dynamically locked MAC.

show port-security static

This command displays the statically locked MAC addresses for port. Instead of slot/port, `lag` *`lag-intf-num`* can be used as an alternate way to specify the LAG interface. `lag` *`lag-intf-num`* can also be used to specify the LAG interface where *`lag-intf-num`* is the LAG port number.

Format	`show port-security static` {`slot/port` | *`lag lag-intf-num`*}
Mode	Privileged EXEC

Term	Definition
Statically Configured MAC Address	The statically configured MAC address.
VLAN ID	The ID of the VLAN that includes the host with the specified MAC address.
Sticky	Indicates whether the static MAC address entry is added in sticky mode.

The following shows example CLI display output for the command.

```
(CN1610) #show port-security static 1/0/1

 Number of static MAC addresses configured: 2

 Statically configured MAC Address    VLAN ID    Sticky
 ---------------------------------    -------    ------
 00:00:00:00:00:01                    2            Yes
 00:00:00:00:00:02                    2            No
```

show port-security violation

This command displays the source MAC address of the last packet discarded on a locked port. Instead of slot/port, `lag` *`lag-intf-num`* can be used as an alternate way to specify the LAG interface. `lag` *`lag-intf-num`* can also be used to specify the LAG interface where *`lag-intf-num`* is the LAG port number.

Format	`show port-security violation {slot/port` | *`lag lag-id}`*
Mode	Privileged EXEC

Term	Definition
MAC Address	The source MAC address of the last frame that was discarded at a locked port.
VLAN ID	The VLAN ID, if applicable, associated with the MAC address of the last frame that was discarded at a locked port.

LLDP (802.1AB) Commands

This section describes the command you use to configure Link Layer Discovery Protocol (LLDP), which is defined in the IEEE 802.1AB specification. LLDP allows stations on an 802 LAN to advertise major capabilities and physical descriptions. The advertisements allow a network management system (NMS) to access and display this information.

lldp transmit

Use this command to enable the LLDP advertise capability on an interface or a range of interfaces.

Default	disabled
Format	`lldp transmit`
Mode	Interface Config

no lldp transmit

Use this command to return the local data transmission capability to the default.

Format	`no lldp transmit`
Mode	Interface Config

lldp receive

Use this command to enable the LLDP receive capability on an interface or a range of interfaces.

Default	disabled
Format	`lldp receive`
Mode	Interface Config

no lldp receive

Use this command to return the reception of LLDPDUs to the default value.

Format	`no lldp receive`

Mode	Interface Config

lldp timers

Use this command to set the timing parameters for local data transmission on ports enabled for LLDP. The *interval-seconds* determines the number of seconds to wait between transmitting local data LLDPDUs. The range is 1-32768 seconds. The *hold-value* is the multiplier on the transmit interval that sets the TTL in local data LLDPDUs. The multiplier range is 2-10. The *reinit-seconds* is the delay before reinitialization, and the range is 1-0 seconds.

Default	◆ interval—30 seconds ◆ hold—4 ◆ reinit—2 seconds
Format	`lldp timers [interval` *`interval-seconds`*`] [hold` *`hold-value`*`] [reinit` *`reinit-seconds`*`]`
Mode	Global Config

no lldp timers

Use this command to return any or all timing parameters for local data transmission on ports enabled for LLDP to the default values.

Format	`no lldp timers [interval] [hold] [reinit]`
Mode	Global Config

lldp transmit-tlv

Use this command to specify which optional type length values (TLVs) in the 802.1AB basic management set are transmitted in the LLDPDUs from an interface or range of interfaces. Use *sys-name* to transmit the system name TLV. To configure the system name, see “snmp-server” on page 89. Use *sys-desc* to transmit the system description TLV. Use *sys-cap* to transmit the system capabilities TLV. Use *port-desc* to transmit the port description TLV. To configure the port description, see “description” on page 310.

Default	no optional TLVs are included
Format	`lldp transmit-tlv [sys-desc] [sys-name] [sys-cap] [port-desc]`
Mode	Interface Config

no lldp transmit-tlv

Use this command to remove an optional TLV from the LLDPDUs. Use the command without parameters to remove all optional TLVs from the LLDPDU.

Format	`no lldp transmit-tlv [sys-desc] [sys-name] [sys-cap] [port-desc]`
Mode	Interface Config

lldp transmit-mgmt

Use this command to include transmission of the local system management address information in the LLDPDUs. This command can be used to configure a single interface or a range of interfaces.

Format	`lldp transmit-mgmt`
Mode	Interface Config

no lldp transmit-mgmt

Use this command to include transmission of the local system management address information in the LLDPDUs. Use this command to cancel inclusion of the management information in LLDPDUs.

Format	`no lldp transmit-mgmt`
Mode	Interface Config

lldp notification

Use this command to enable remote data change notifications on an interface or a range of interfaces.

Default	disabled
Format	`lldp notification`
Mode	Interface Config

no lldp notification

Use this command to disable notifications.

Default	disabled

Format	`no lldp notification`
Mode	Interface Config

lldp notification-interval

Use this command to configure how frequently the system sends remote data change notifications. The *interval* parameter is the number of seconds to wait between sending notifications. The valid interval range is 5-3600 seconds.

Default	5
Format	`lldp notification-interval` *interval*
Mode	Global Config

no lldp notification-interval

Use this command to return the notification interval to the default value.

Format	`no lldp notification-interval`
Mode	Global Config

clear lldp statistics

Use this command to reset all LLDP statistics, including MED-related information.

Format	`clear lldp statistics`
Mode	Privileged EXEC

clear lldp remote-data

Use this command to delete all information from the LLDP remote data table, including MED-related information.

Format	`clear lldp remote-data`
Mode	Global Config

show lldp

Use this command to display a summary of the current LLDP configuration.

Format	`show lldp`
Mode	Privileged EXEC

Term	Definition
Transmit Interval	How frequently the system transmits local data LLDPDUs, in seconds.
Transmit Hold Multiplier	The multiplier on the transmit interval that sets the TTL in local data LLDPDUs.
Re-initialization Delay	The delay before reinitialization, in seconds.
Notification Interval	How frequently the system sends remote data change notifications, in seconds.

show lldp interface

Use this command to display a summary of the current LLDP configuration for a specific interface or for all interfaces.

Format	`show lldp interface {slot/port | all}`
Mode	Privileged EXEC

Term	Definition
Interface	The interface in a slot/port format.
Link	Shows whether the link is up or down.
Transmit	Shows whether the interface transmits LLDPDUs.
Receive	Shows whether the interface receives LLDPDUs.
Notify	Shows whether the interface sends remote data change notifications.

Term	Definition
TLVs	Shows whether the interface sends optional TLVs in the LLDPDUs. The TLV codes can be 0 (Port Description), 1 (System Name), 2 (System Description), or 3 (System Capability).
Mgmt	Shows whether the interface transmits system management address information in the LLDPDUs.

show lldp statistics

Use this command to display the current LLDP traffic and remote table statistics for a specific interface or for all interfaces.

Format	`show lldp statistics {slot/port | all}`
Mode	Privileged EXEC

Term	Definition
Last Update	The amount of time since the last update to the remote table in days, hours, minutes, and seconds.
Total Inserts	Total number of inserts to the remote data table.
Total Deletes	Total number of deletes from the remote data table.
Total Drops	Total number of times the complete remote data received was not inserted due to insufficient resources.
Total Ageouts	Total number of times a complete remote data entry was deleted because the Time to Live interval expired.

The table contains the following column headings:

Term	Definition
Interface	The interface in slot/port format.

Term	Definition
TX Total	Total number of LLDP packets transmitted on the port.
RX Total	Total number of LLDP packets received on the port.
Discards	Total number of LLDP frames discarded on the port for any reason.
Errors	The number of invalid LLDP frames received on the port.
Ageouts	Total number of times a complete remote data entry was deleted for the port because the Time to Live interval expired.
TVL Discards	The number of TLVs discarded.
TVL Unknowns	Total number of LLDP TLVs received on the port where the type value is in the reserved range, and not recognized.
TLV MED	The total number of LLDP-MED TLVs received on the interface.
TLV 802.1	The total number of LLDP TLVs received on the interface which are of type 802.1.
TLV 802.3	The total number of LLDP TLVs received on the interface which are of type 802.3.

show lldp remote-device

Use this command to display summary information about remote devices that transmit current LLDP data to the system. You can show information about LLDP remote data received on all ports or on a specific port.

Format	`show lldp remote-device {slot/port | all}`
Mode	Privileged EXEC

Term	Definition
Local Interface	The interface that received the LLDPDU from the remote device.
RemID	An internal identifier to the switch to mark each remote device to the system.
Chassis ID	The ID that is sent by a remote device as part of the LLDP message, it is usually a MAC address of the device.
Port ID	The port number that transmitted the LLDPDU.
System Name	The system name of the remote device.

The following shows example CLI display output for the command.

```
(FASTPATH Switching) #show lldp remote-device all

LLDP Remote Device Summary

Local
Interface RemID    Chassis ID            Port ID             System
Name
-------  -------   --------------------  ------------------  ------
------------
0/1
0/2
0/3
0/4
0/5
0/6
0/7        2       00:FC:E3:90:01:0F     00:FC:E3:90:01:11
0/7        3       00:FC:E3:90:01:0F     00:FC:E3:90:01:12
0/7        4       00:FC:E3:90:01:0F     00:FC:E3:90:01:13
0/7        5       00:FC:E3:90:01:0F     00:FC:E3:90:01:14
0/7        1       00:FC:E3:90:01:0F     00:FC:E3:90:03:11
0/7        6       00:FC:E3:90:01:0F     00:FC:E3:90:04:11
0/8
0/9
0/10
0/11
0/12
--More-- or (q)uit
```

show lldp remote-device detail

Use this command to display detailed information about remote devices that transmit current LLDP data to an interface on the system.

Format	`show lldp remote-device detail slot/port`
Mode	Privileged EXEC

Term	Definition
Local Interface	The interface that received the LLDPDU from the remote device.
Remote Identifier	An internal identifier to the switch to mark each remote device to the system.
Chassis ID Subtype	The type of identification used in the Chassis ID field.
Chassis ID	The chassis of the remote device.
Port ID Subtype	The type of port on the remote device.
Port ID	The port number that transmitted the LLDPDU.
System Name	The system name of the remote device.
System Description	Describes the remote system by identifying the system name and versions of hardware, operating system, and networking software supported in the device.
Port Description	Describes the port in an alpha-numeric format. The port description is configurable.
System Capabilities Supported	Indicates the primary function(s) of the device.
System Capabilities Enabled	Shows which of the supported system capabilities are enabled.
Management Address	For each interface on the remote device with an LLDP agent, lists the type of address the remote LLDP agent uses and specifies the address used to obtain information related to the device.

Term	Definition
Time To Live	The amount of time (in seconds) the remote device's information received in the LLDPDU should be treated as valid information.

The following shows example CLI display output for the command.

```
(FASTPATH Switching) #show lldp remote-device detail 0/7

LLDP Remote Device Detail

Local Interface: 0/7


Remote Identifier: 2
Chassis ID Subtype: MAC Address
Chassis ID: 00:FC:E3:90:01:0F
Port ID Subtype: MAC Address
Port ID: 00:FC:E3:90:01:11
System Name:
System Description:
Port Description:
System Capabilities Supported:
System Capabilities Enabled:
Time to Live: 24 seconds
```

show lldp local-device

Use this command to display summary information about the advertised LLDP local data. This command can display summary information or detail for each interface.

Format	`show lldp local-device {slot/port | all}`
Mode	Privileged EXEC

Term	Definition
Interface	The interface in a slot/port format.
Port ID	The port ID associated with this interface.
Port Description	The port description associated with the interface.

show lldp local-device detail

Use this command to display detailed information about the LLDP data a specific interface transmits.

Format	`show lldp local-device detail slot/port`
Mode	Privileged EXEC

Term	Definition
Interface	The interface that sends the LLDPDU.
Chassis ID Subtype	The type of identification used in the Chassis ID field.
Chassis ID	The chassis of the local device.
Port ID Subtype	The type of port on the local device.
Port ID	The port number that transmitted the LLDPDU.
System Name	The system name of the local device.
System Description	Describes the local system by identifying the system name and versions of hardware, operating system, and networking software supported in the device.
Port Description	Describes the port in an alpha-numeric format.
System Capabilities Supported	Indicates the primary function(s) of the device.
System Capabilities Enabled	Shows which of the supported system capabilities are enabled.
Management Address	The type of address and the specific address the local LLDP agent uses to send and receive information.

LLDP-MED Commands

Link Layer Discovery Protocol - Media Endpoint Discovery (LLDP-MED) (ANSI-TIA-1057) provides an extension to the LLDP standard. Specifically, LLDP-MED provides extensions for network configuration and policy, device location, Power over Ethernet (PoE) management and inventory management.

lldp med

Use this command to enable MED on an interface or a range of interfaces. By enabling MED, you will be effectively enabling the transmit and receive function of LLDP.

Default	disabled
Format	`lldp med`
Mode	Interface Config

no lldp med

Use this command to disable MED.

Format	`no lldp med`
Mode	Interface Config

lldp med configNotification

Use this command to configure an interface or a range of interfaces to send the topology change notification.

Default	disabled
Format	`lldp med configNotification`
Mode	Interface Config

no ldp med configNotification

Use this command to disable notifications.

Format	`no lldp med configNotification`
Mode	Interface Config

lldp med transmit-tlv

Use this command to specify which optional Type Length Values (TLVs) in the LLDP MED set will be transmitted in the Link Layer Discovery Protocol Data Units (LLDPDUs) from this interface or a range of interfaces.

Default	By default, the capabilities and network policy TLVs are included.
Format	`lldp med transmit-tlv [capabilities] [ex-pd] [ex-pse] [inventory] [location] [network-policy]`
Mode	Interface Config

Term	Definition
capabilities	Transmit the LLDP capabilities TLV.
ex-pd	Transmit the LLDP extended PD TLV.
ex-pse	Transmit the LLDP extended PSE TLV.
inventory	Transmit the LLDP inventory TLV.
location	Transmit the LLDP location TLV.
network-policy	Transmit the LLDP network policy TLV.

no lldp med transmit-tlv

Use this command to remove a TLV.

Format	`no lldp med transmit-tlv [capabilities] [network-policy] [ex-pse] [ex-pd] [location] [inventory]`
Mode	Interface Config

lldp med all

Use this command to configure LLDP-MED on all the ports.

Format	`lldp med all`
Mode	Global Config

lldp med confignotification all

Use this command to configure all the ports to send the topology change notification.

Format	`lldp med confignotification all`
Mode	Global Config

lldp med faststartrepeatcount

Use this command to set the value of the fast start repeat count. *[count]* is the number of LLDP PDUs that will be transmitted when the product is enabled. The range is 1 to 10.

Default	3
Format	`lldp med faststartrepeatcount` *[count]*
Mode	Global Config

no lldp med faststartrepeatcount

Use this command to return to the factory default value.

Format	`no lldp med faststartrepeatcount`
Mode	Global Config

lldp med transmit-tlv all

Use this command to specify which optional Type Length Values (TLVs) in the LLDP MED set will be transmitted in the Link Layer Discovery Protocol Data Units (LLDPDUs).

Default	By default, the capabilities and network policy TLVs are included.
Format	`lldp med transmit-tlv all [capabilities] [ex-pd] [ex-pse] [inventory] [location] [network-policy]`
Mode	Global Config

Term	Definition
capabilities	Transmit the LLDP capabilities TLV.
ex-pd	Transmit the LLDP extended PD TLV.

Term	Definition
ex-pse	Transmit the LLDP extended PSE TLV.
inventory	Transmit the LLDP inventory TLV.
location	Transmit the LLDP location TLV.
network-policy	Transmit the LLDP network policy TLV.

no lldp med transmit-tlv

Use this command to remove a TLV.

Format	`no lldp med transmit-tlv [capabilities] [network-policy] [ex-pse] [ex-pd] [location] [inventory]`
Mode	Global Config

show lldp med

Use this command to display a summary of the current LLDP MED configuration.

Format	`show lldp med`
Mode	Privileged EXEC

The following shows example CLI display output for the command.

```
(CN1610) #show lldp med
LLDP MED Global Configuration

Fast Start Repeat Count: 3
Device Class: Network Connectivity

(CN1610) #
```

show lldp med interface

Use this command to display a summary of the current LLDP MED configuration for a specific interface. *unit/slot/port* indicates a specific physical interface. *all* indicates all valid LLDP interfaces.

Format	`show lldp med interface {`*unit/slot/port* `| all}`

Mode	Privileged EXEC

The following shows example CLI display output for the command.

```
(CN1610) #show lldp med interface all

Interface  Link    configMED operMED   ConfigNotify TLVsTx
---------  ------  --------- --------  ------------ -----------
1/0/1      Down    Disabled  Disabled  Disabled     0,1
1/0/2      Up      Disabled  Disabled  Disabled     0,1
1/0/3      Down    Disabled  Disabled  Disabled     0,1
1/0/4      Down    Disabled  Disabled  Disabled     0,1
1/0/5      Down    Disabled  Disabled  Disabled     0,1
1/0/6      Down    Disabled  Disabled  Disabled     0,1
1/0/7      Down    Disabled  Disabled  Disabled     0,1
1/0/8      Down    Disabled  Disabled  Disabled     0,1
1/0/9      Down    Disabled  Disabled  Disabled     0,1
1/0/10     Down    Disabled  Disabled  Disabled     0,1
1/0/11     Down    Disabled  Disabled  Disabled     0,1
1/0/12     Down    Disabled  Disabled  Disabled     0,1
1/0/13     Down    Disabled  Disabled  Disabled     0,1
1/0/14     Down    Disabled  Disabled  Disabled     0,1

TLV Codes: 0- Capabilities,       1- Network Policy
           2- Location,           3- Extended PSE
           4- Extended Pd,        5- Inventory
--More-- or (q)uit
(CN1610) #show lldp med interface 1/0/2

Interface  Link    configMED operMED   ConfigNotify TLVsTx
---------  ------  --------- --------  ------------ -----------
1/0/2      Up      Disabled  Disabled  Disabled     0,1

TLV Codes: 0- Capabilities,       1- Network Policy
           2- Location,           3- Extended PSE
           4- Extended Pd,        5- Inventory

(CN1610) #
```

show lldp med local-device detail

Use this command to display detailed information about the LLDP MED data that a specific interface transmits. slot/port indicates a specific physical interface.

Format	`show lldp med local-device detail slot/port`

Mode	Privileged EXEC

The following shows example CLI display output for the command.

```
(CN1610) #show lldp med local-device detail 1/0/8

LLDP MED Local Device Detail

Interface: 1/0/8

Network Policies
Media Policy Application Type : voice
Vlan ID: 10
Priority: 5
DSCP: 1
Unknown: False
Tagged: True

Media Policy Application Type : streamingvideo
Vlan ID: 20
Priority: 1
DSCP: 2
Unknown: False
Tagged: True

Inventory
Hardware Rev: xxx xxx xxx
Firmware Rev: xxx xxx xxx
Software Rev: xxx xxx xxx
Serial Num: xxx xxx xxx
Mfg Name: xxx xxx xxx
Model Name: xxx xxx xxx
Asset ID: xxx xxx xxx

Location
Subtype: elin
Info: xxx xxx xxx

Extended POE
Device Type: pseDevice

Extended POE PSE
Available: 0.3 Watts
Source: primary
Priority: critical

Extended POE PD
```

```
Required: 0.2 Watts
Source: local
Priority: low
```

show lldp med remote-device

Use this command to display the summary information about remote devices that transmit current LLDP MED data to the system. You can show information about LLDP MED remote data received on all valid LLDP interfaces or on a specific physical interface.

Format	`show lldp med remote-device {slot/port | all}`
Mode	Privileged EXEC

Term	Definition
Local Interface	The interface that received the LLDPDU from the remote device.
Remote ID	An internal identifier to the switch to mark each remote device to the system.
Device Class	Device classification of the remote device.

The following shows example CLI display output for the command.

```
(CN1610) #show lldp med remote-device all

LLDP MED Remote Device Summary

Local
Interface  Remote ID  Device Class
---------  ---------  ------------
1/0/8 1Class I
1/0/9 2Not Defined
1/0/10 3Class II
1/0/11 4Class III
1/0/12 5    Network Con
```

show lldp med remote-device detail

Use this command to display detailed information about remote devices that transmit current LLDP MED data to an interface on the system.

Format	`show lldp med remote-device detail slot/port`
Mode	Privileged EXEC

The following shows example CLI display output for the command.

```
(CN1610) #show lldp med remote-device detail 1/0/8

LLDP MED Remote Device Detail

Local Interface: 1/0/8
Remote Identifier: 18
Capabilities
MED Capabilities Supported: capabilities, networkpolicy, location,
extendedpse
MED Capabilities Enabled: capabilities, networkpolicy
Device Class: Endpoint Class I

Network Policies
Media Policy Application Type : voice
Vlan ID: 10
Priority: 5
DSCP: 1
Unknown: False
Tagged: True

Media Policy Application Type : streamingvideo
Vlan ID: 20
Priority: 1
DSCP: 2
Unknown: False
Tagged: True


Inventory
Hardware Rev: xxx xxx xxx
Firmware Rev: xxx xxx xxx
Software Rev: xxx xxx xxx
Serial Num: xxx xxx xxx
Mfg Name: xxx xxx xxx
Model Name: xxx xxx xxx
Asset ID: xxx xxx xxx

Location
```

```
Subtype: elin
Info: xxx xxx xxx

Extended POE
Device Type: pseDevice

Extended POE PSE
Available: 0.3 Watts
Source: primary
Priority: critical

Extended POE PD

Required: 0.2 Watts
Source: local
Priority: low
```

Denial of Service Commands

This section describes the commands you use to configure Denial of Service (DoS) Control. FASTPATH software provides support for classifying and blocking specific types of Denial of Service attacks. You can configure your system to monitor and block these types of attacks:

- **SIP = DIP:** Source IP address = Destination IP address.
- **First Fragment:**TCP Header size smaller then configured value.
- **TCP Fragment:** Allows the device to drop packets that have a TCP payload where the IP payload length minus the IP header size is less than the minimum allowed TCP header size.
- **TCP Flag:** TCP Flag SYN set and Source Port < 1024 or TCP Control Flags = 0 and TCP Sequence Number = 0 or TCP Flags FIN, URG, and PSH set and TCP Sequence Number = 0 or TCP Flags SYN and FIN set.
- **L4 Port:** Source TCP/UDP Port = Destination TCP/UDP Port.
- **ICMP:** Limiting the size of ICMP Ping packets.
- **SMAC = DMAC:** Source MAC address = Destination MAC address
- **TCP Port:** Source TCP Port = Destination TCP Port
- **UDP Port**: Source UDP Port = Destination UDP Port
- **TCP Flag & Sequence:** TCP Flag SYN set and Source Port < 1024 or TCP Control Flags = 0 and TCP Sequence Number = 0 or TCP Flags FIN, URG, and PSH set and TCP Sequence Number = 0 or TCP Flags SYN and FIN set.
- **TCP Offset:** Allows the device to drop packets that have a TCP header Offset set to 1.
- **TCP SYN:** TCP Flag SYN set.
- **TCP SYN & FIN:** TCP Flags SYN and FIN set.
- **TCP FIN & URG & PSH:** TCP Flags FIN and URG and PSH set and TCP Sequence Number = 0.
- **ICMP V6**: Limiting the size of ICMPv6 Ping packets.
- **ICMP Fragment**: Checks for fragmented ICMP packets.

dos-control all

This command enables Denial of Service protection checks globally.

Default	disabled
Format	`dos-control all`

Mode	Global Config

no dos-control all

This command disables Denial of Service prevention checks globally.

Format	`no dos-control all`
Mode	Global Config

dos-control sipdip

This command enables Source IP address = Destination IP address (SIP = DIP) Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress with SIP = DIP, the packets will be dropped if the mode is enabled.

Default	disabled
Format	`dos-control sipdip`
Mode	Global Config

no dos-control sipdip

This command disables Source IP address = Destination IP address (SIP = DIP) Denial of Service prevention.

Format	`no dos-control sipdip`
Mode	Global Config

dos-control firstfrag

This command enables Minimum TCP Header Size Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having a TCP Header Size smaller then the configured value, the packets will be dropped if the mode is enabled.The default is *disabled*. If you enable dos-control firstfrag, but do not provide a Minimum TCP Header Size, the system sets that value to *20*.

Default	disabled (20)
Format	`dos-control firstfrag [`*0-255*`]`

Mode	Global Config

no dos-control firstfrag

This command sets Minimum TCP Header Size Denial of Service protection to the default value of *disabled*.

Format	`no dos-control firstfrag`
Mode	Global Config

dos-control tcpfrag

This command enables TCP Fragment Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack and packets that have a TCP payload in which the IP payload length minus the IP header size is less than the minimum allowed TCP header size are dropped.

Default	disabled
Format	`dos-control tcpfrag`
Mode	Global Config

no dos-control tcpfrag

This command disables TCP Fragment Denial of Service protection.

Format	`no dos-control tcpfrag`
Mode	Global Config

dos-control tcpflag

This command enables TCP Flag Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attacks. If packets ingress having TCP Flag SYN set and a source port less than 1024 or having TCP Control Flags set to 0 and TCP Sequence Number set to 0 or having TCP Flags FIN, URG, and PSH set and TCP Sequence Number set to 0 or having TCP Flags SYN and FIN both set, the packets will be dropped if the mode is enabled.

Default	disabled
Format	`dos-control tcpflag`

Mode	Global Config

no dos-control tcpflag

This command sets disables TCP Flag Denial of Service protections.

Format	`no dos-control tcpflag`
Mode	Global Config

dos-control l4port

This command enables L4 Port Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having Source TCP/UDP Port Number equal to Destination TCP/UDP Port Number, the packets will be dropped if the mode is enabled.

Note

Some applications mirror source and destination L4 ports - RIP for example uses 520 for both. If you enable dos-control l4port, applications such as RIP may experience packet loss which would render the application inoperable.

Default	disabled
Format	`dos-control l4port`
Mode	Global Config

no dos-control l4port

This command disables L4 Port Denial of Service protections.

Format	`no dos-control l4port`
Mode	Global Config

dos-control smacdmac

This command enables Source MAC address = Destination MAC address (SMAC = DMAC) Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress with SMAC = DMAC, the packets will be dropped if the mode is enabled.

Default	disabled

Format	`dos-control smacdmac`
Mode	Global Config

no dos-control smacdmac

This command disables Source MAC address = Destination MAC address (SMAC = DMAC) DoS protection.

Format	`no dos-control smacdmac`
Mode	Global Config

dos-control tcpport

This command enables TCP L4 source = destination port number (Source TCP Port = Destination TCP Port) Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress with Source TCP Port = Destination TCP Port, the packets will be dropped if the mode is enabled.

Default	disabled
Format	`dos-control tcpport`
Mode	Global Config

no dos-control tcpport

This command disables TCP L4 source = destination port number (Source TCP Port = Destination TCP Port) Denial of Service protection.

Format	`no dos-control tcpport`
Mode	Global Config

dos-control udpport

This command enables UDP L4 source = destination port number (Source UDP Port = Destination UDP Port) DoS protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress with Source UDP Port = Destination UDP Port, the packets will be dropped if the mode is enabled.

Default	disabled
Format	`dos-control udpport`
Mode	Global Config

no dos-control udpport

This command disables UDP L4 source = destination port number (Source UDP Port = Destination UDP Port) Denial of Service protection.

Format	`no dos-control udpport`
Mode	Global Config

dos-control tcpflagseq

This command enables TCP Flag and Sequence Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having TCP Flag SYN set and a source port less than 1024 or having TCP Control Flags set to 0 and TCP Sequence Number set to 0 or having TCP Flags FIN, URG, and PSH set and TCP Sequence Number set to 0 or having TCP Flags SYN and FIN both set, the packets will be dropped if the mode is enabled.

Default	disabled
Format	`dos-control tcpflagseq`
Mode	Global Config

no dos-control tcpflagseq

This command sets disables TCP Flag and Sequence Denial of Service protection.

Format	`no dos-control tcpflagseq`
Mode	Global Config

dos-control tcpoffset

This command enables TCP Offset Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having TCP Header Offset equal to one (1), the packets will be dropped if the mode is enabled.

Default	disabled
Format	`dos-control tcpoffset`
Mode	Global Config

no dos-control tcpoffset

This command disabled TCP Offset Denial of Service protection.

Format	`no dos-control tcpoffset`
Mode	Global Config

dos-control tcpsyn

This command enables TCP SYN and L4 source = 0-1023 Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having TCP flag SYN set and an L4 source port from 0 to 1023, the packets will be dropped if the mode is enabled.

Default	disabled
Format	`dos-control tcpsyn`
Mode	Global Config

no dos-control tcpsyn

This command sets disables TCP SYN and L4 source = 0-1023 Denial of Service protection.

Format	`no dos-control tcpsyn`
Mode	Global Config

dos-control tcpsynfin

This command enables TCP SYN and FIN Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having TCP flags SYN and FIN set, the packets will be dropped if the mode is enabled.

Default	disabled
Format	`dos-control tcpsynfin`
Mode	Global Config

no dos-control tcpsynfin

This command sets disables TCP SYN & FIN Denial of Service protection.

Format	`no dos-control tcpsynfin`
Mode	Global Config

dos-control tcpfinurgpsh

This command enables TCP FIN and URG and PSH and SEQ = 0 checking Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having TCP FIN, URG, and PSH all set and TCP Sequence Number set to 0, the packets will be dropped if the mode is enabled.

Default	disabled
Format	`dos-control tcpfinurgpsh`
Mode	Global Config

no dos-control tcpfinurgpsh

This command sets disables TCP FIN and URG and PSH and SEQ = 0 checking Denial of Service protections.

Format	`no dos-control tcpfinurgpsh`
Mode	Global Config

dos-control icmpv4

This command enables Maximum ICMPv4 Packet Size Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attack. If ICMPv4 Echo Request (PING) packets ingress having a size greater than the configured value, the packets will be dropped if the mode is enabled.

Default	disabled (512)
Format	`dos-control icmpv4 [0-16376]`
Mode	Global Config

no dos-control icmpv4

This command disables Maximum ICMP Packet Size Denial of Service protections.

Format	`no dos-control icmpv4`
Mode	Global Config

dos-control icmpv6

This command enables Maximum ICMPv6 Packet Size Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attack. If ICMPv6 Echo Request (PING) packets ingress having a size greater than the configured value, the packets will be dropped if the mode is enabled.

Default	disabled (512)
Format	`dos-control icmpv6 0-16376`
Mode	Global Config

no dos-control icmpv6

This command disables Maximum ICMP Packet Size Denial of Service protections.

Format	`no dos-control icmpv6`
Mode	Global Config

dos-control icmpfrag

This command enables ICMP Fragment Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having fragmented ICMP packets, the packets will be dropped if the mode is enabled.

Default	disabled
Format	`dos-control icmpfrag`
Mode	Global Config

no dos-control icmpfrag

This command disabled ICMP Fragment Denial of Service protection.

Format	`no dos-control icmpfrag`
Mode	Global Config

show dos-control

This command displays Denial of Service configuration information.

Format	`show dos-control`
Mode	Privileged EXEC

Term	Definition
First Fragment Mode	The administrative mode of First Fragment DoS prevention. When enabled, this causes the switch to drop packets that have a TCP header smaller then the configured Min TCP Hdr Size.
Min TCP Hdr Size	The minimum TCP header size the switch will accept if First Fragment DoS prevention is enabled.
ICMPv4 Mode	The administrative mode of ICMPv4 DoS prevention. When enabled, this causes the switch to drop ICMP packets that have a type set to ECHO_REQ (ping) and a size greater than the configured ICMPv4 Payload Size.

Term	Definition
Max ICMPv4 Payload Size	The maximum ICMPv4 payload size to accept when ICMPv4 DoS protection is enabled.
ICMPv6 Mode	The administrative mode of ICMPv6 DoS prevention. When enabled, this causes the switch to drop ICMP packets that have a type set to ECHO_REQ (ping) and a size greater than the configured ICMPv6 Payload Size.
Max ICMPv6 Payload Size	The maximum ICMPv6 payload size to accept when ICMPv6 DoS protection is enabled.
ICMPv4 Fragment Mode	The administrative mode of ICMPv4 Fragment DoS prevention. When enabled, this causes the switch to drop fragmented ICMPv4 packets.
TCP Port Mode	The administrative mode of TCP Port DoS prevention. When enabled, this causes the switch to drop packets that have the TCP source port equal to the TCP destination port.
UDP Port Mode	The administrative mode of UDP Port DoS prevention. When enabled, this causes the switch to drop packets that have the UDP source port equal to the UDP destination port.
SIPDIP Mode	The administrative mode of SIP=DIP DoS prevention. Enabling this causes the switch to drop packets that have a source IP address equal to the destination IP address. The factory default is disabled.
SMACDMAC Mode	The administrative mode of SMAC=DMAC DoS prevention. Enabling this causes the switch to drop packets that have a source MAC address equal to the destination MAC address.
TCP FIN&URG& PSH Mode	The administrative mode of TCP FIN & URG & PSH DoS prevention. Enabling this causes the switch to drop packets that have TCP flags FIN, URG, and PSH set and TCP Sequence Number = 0.

Term	Definition
Max ICMPv4 Payload Size	The maximum ICMPv4 payload size to accept when ICMPv4 DoS protection is enabled.
ICMPv6 Mode	The administrative mode of ICMPv6 DoS prevention. When enabled, this causes the switch to drop ICMP packets that have a type set to ECHO_REQ (ping) and a size greater than the configured ICMPv6 Payload Size.
Max ICMPv6 Payload Size	The maximum ICMPv6 payload size to accept when ICMPv6 DoS protection is enabled.
ICMPv4 Fragment Mode	The administrative mode of ICMPv4 Fragment DoS prevention. When enabled, this causes the switch to drop fragmented ICMPv4 packets.
TCP Port Mode	The administrative mode of TCP Port DoS prevention. When enabled, this causes the switch to drop packets that have the TCP source port equal to the TCP destination port.
UDP Port Mode	The administrative mode of UDP Port DoS prevention. When enabled, this causes the switch to drop packets that have the UDP source port equal to the UDP destination port.
SIPDIP Mode	The administrative mode of SIP=DIP DoS prevention. Enabling this causes the switch to drop packets that have a source IP address equal to the destination IP address. The factory default is disabled.
SMACDMAC Mode	The administrative mode of SMAC=DMAC DoS prevention. Enabling this causes the switch to drop packets that have a source MAC address equal to the destination MAC address.
TCP FIN&URG& PSH Mode	The administrative mode of TCP FIN & URG & PSH DoS prevention. Enabling this causes the switch to drop packets that have TCP flags FIN, URG, and PSH set and TCP Sequence Number = 0.

Term	Definition
TCP Flag & Sequence Mode	The administrative mode of TCP Flag DoS prevention. Enabling this causes the switch to drop packets that have TCP control flags set to 0 and TCP sequence number set to 0.
TCP SYN Mode	The administrative mode of TCP SYN DoS prevention. Enabling this causes the switch to drop packets that have TCP Flags SYN set.
TCP SYN & FIN Mode	The administrative mode of TCP SYN & FIN DoS prevention. Enabling this causes the switch to drop packets that have TCP Flags SYN and FIN set.
TCP Fragment Mode	The administrative mode of TCP Fragment DoS prevention. Enabling this causes the switch to drop packets that have a TCP payload in which the IP payload length minus the IP header size is less than the minimum allowed TCP header size.
TCP Offset Mode	The administrative mode of TCP Offset DoS prevention. Enabling this causes the switch to drop packets that have a TCP header Offset equal to 1.

MAC Database Commands

This section describes the commands you use to configure and view information about the MAC databases.

bridge aging-time

This command configures the forwarding database address aging timeout in seconds. The *seconds* parameter must be within the range of 10 to 1,000,000 seconds. In an SVL system, the [fdbid/all] parameter is not used and will be ignored if entered. In an SVL system, the [fdbid/all] parameter is not used and will be ignored if entered.

Default	300
Format	`bridge aging-time` *`10-1,000,000`*
Mode	Global Config

no bridge aging-time

This command sets the forwarding database address aging timeout to the default value. In an SVL system, the [fdbid/all] parameter is not used and will be ignored if entered.

Format	`no bridge aging-time`
Mode	Global Config

show forwardingdb agetime

This command displays the timeout for address aging.

Default	all
Format	`show forwardingdb agetime`
Mode	Privileged EXEC

Term	Definition
Address Aging Timeout	Displays the system's address aging timeout value in seconds.

show mac-address-table multicast

This command displays the Multicast Forwarding Database (MFDB) information. If you enter the command with no parameter, the entire table is displayed. You can display the table entry for one MAC Address by specifying the MAC address as an optional parameter.

Format	`show mac-address-table multicast` *macaddr*
Mode	Privileged EXEC

Term	Definition
VLAN ID	The VLAN in which the MAC address is learned.
MAC Address	A multicast MAC address for which the switch has forwarding or filtering information. The format is 6 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB.
Source	The component that is responsible for this entry in the Multicast Forwarding Database. The source can be IGMP Snooping, GMRP, and Static Filtering.
Type	The type of the entry. Static entries are those that are configured by the end user. Dynamic entries are added to the table as a result of a learning process or protocol.
Description	The text description of this multicast table entry.
Interfaces	The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).

Term	Definition
Fwd Interface	The resultant forwarding list is derived from combining all the component's forwarding interfaces and removing the interfaces that are listed as the static filtering interfaces.

If one or more entries exist in the multicast forwarding table, the command output looks similar to the following:

```
(CN1610) #show mac-address-table multicast


                                        Fwd
VLAN ID MAC Address       Source  Type    Description     Interface
Interface
------- ----------------- ------- ------- --------------- ---------
---------
1       01:00:5E:01:02:03 Filter  Static  Mgmt Config     Fwd:
Fwd:

1/0/1,    1/0/1,

1/0/2,    1/0/2,

1/0/3,    1/0/3,

                                          1/0/4,    1/0/4,

1/0/5,    1/0/5,

1/0/6,    1/0/6,

          1/0/7,    1/0/7,

1/0/8,    1/0/8,

1/0/9,    1/0/9,

1/0/10,   1/0/10,
--More-- or (q)uit
```

show mac-address-table stats This command displays the Multicast Forwarding Database (MFDB) statistics.

Format	`show mac-address-table stats`
Mode	Privileged EXEC

Term	Definition
Total Entries	The total number of entries that can possibly be in the Multicast Forwarding Database table.
Most MFDB Entries Ever Used	The largest number of entries that have been present in the Multicast Forwarding Database table. This value is also known as the MFDB high-water mark.
Current Entries	The current number of entries in the MFDB.

ISDP Commands

This section describes the commands you use to configure the industry standard Discovery Protocol (ISDP).

isdp run

This command enables ISDP on the switch.

Default	Enabled
Format	`isdp run`
Mode	Global Config

no isdp run

This command disables ISDP on the switch.

Format	`no isdp run`
Mode	Global Config

isdp holdtime

This command configures the hold time for ISDP packets that the switch transmits. The hold time specifies how long a receiving device should store information sent in the ISDP packet before discarding it. The range is given in seconds.

Default	180 seconds
Format	`isdp holdtime` *`10-255`*
Mode	Global Config

isdp timer

This command sets the period of time between sending new ISDP packets. The range is given in seconds.

Default	60 seconds
Format	`isdp timer` *`5-254`*
Mode	Global Config

isdp advertise-v2

This command enables the sending of ISDP version 2 packets from the device.

Default	Enabled
Format	`isdp advertise-v2`
Mode	Global Config

no isdp advertise-v2

This command disables the sending of ISDP version 2 packets from the device.

Format	`no isdp advertise-v2`
Mode	Global Config

isdp enable

This command enables ISDP on an interface or range of interfaces.

Note

ISDP must be enabled both globally and on the interface in order for the interface to transmit ISDP packets. If ISDP is globally disabled on the switch, the interface will not transmit ISDP packets, regardless of the ISDP status on the interface. To enable ISDP globally, use the command "isdp run" on page 583.

Default	Enabled
Format	`isdp enable`
Mode	Interface Config

no isdp enable

This command disables ISDP on the interface.

Format	`no isdp enable`
Mode	Interface Config

clear isdp counters

This command clears ISDP counters.

Format	`clear isdp counters`
Mode	Privileged EXEC

clear isdp table

This command clears entries in the ISDP table.

Format	`clear isdp table`
Mode	Privileged EXEC

show isdp

This command displays global ISDP settings.

Format	`show isdp`
Mode	Privileged EXEC

Term	Definition
Timer	The frequency with which this device sends ISDP packets. This value is given in seconds.
Hold Time	The length of time the receiving device should save information sent by this device. This value is given in seconds.
Version 2 Advertisements	The setting for sending ISDPv2 packets. If disabled, version 1 packets are transmitted.
Neighbors table time since last change	The amount of time that has passed since the ISPD neighbor table changed.
Device ID	The Device ID advertised by this device. The format of this Device ID is characterized by the value of the Device ID Format object.
Device ID Format Capability	Indicates the Device ID format capability of the device. ◆ *serialNumber* indicates that the device uses a serial number as the format for its Device ID. ◆ *macAddress* indicates that the device uses a Layer 2 MAC address as the format for its Device ID. ◆ *other* indicates that the device uses its platform-specific format as the format for its Device ID.

Term	Definition
Device ID Format	Indicates the Device ID format of the device. ◆ *serialNumber* indicates that the value is in the form of an ASCII string containing the device serial number. ◆ *macAddress* indicates that the value is in the form of a Layer 2 MAC address. ◆ *other* indicates that the value is in the form of a platform specific ASCII string containing info that identifies the device. For example, ASCII string contains serialNumber appended/prepended with system name.

The following shows example CLI display output for the command.

```
(CN1610) #show isdp

Timer..................................... 30
Hold Time................................. 180
Version 2 Advertisements.................. Enabled
Neighbors table time since last change..... 0 days 00:00:00
Device ID................................. 1114728
Device ID format capability............... Serial Number, Host
Name
Device ID format.......................... Serial Number
```

show isdp interface

This command displays ISDP settings for the specified interface.

Format	`show isdp interface {all | slot/port}`
Mode	Privileged EXEC

Term	Definition
Interface	The slot/port of the specified interface.
Mode	ISDP mode enabled/disabled status for the interface(s).

The following shows example CLI display output for the command.

```
(CN1610) #show isdp interface 0/1

Interface        Mode
---------------  ----------
0/1              Enabled
```

The following shows example CLI display output for the command.

```
(Switching) #show isdp interface all

Interface        Mode
---------------  ----------

0/1                 Enabled

0/2                 Enabled

0/3                 Enabled

0/4                 Enabled

0/5                 Enabled

0/6                 Enabled

0/7                 Enabled

0/8                 Enabled
```

show isdp entry

This command displays ISDP entries. If the device id is specified, then only entries for that device are shown.

Format	`show isdp entry {all | deviceid}`
Mode	Privileged EXEC

Term	Definition
Device ID	The device ID associated with the neighbor which advertised the information.
IP Addresses	The IP address(es) associated with the neighbor.

Term	Definition
Capability	ISDP Functional Capabilities advertised by the neighbor.
Platform	The hardware platform advertised by the neighbor.
Interface	The interface (slot/port) on which the neighbor's advertisement was received.
Port ID	The port ID of the interface from which the neighbor sent the advertisement.
Hold Time	The hold time advertised by the neighbor.
Version	The software version that the neighbor is running.
Advertisement Version	The version of the advertisement packet received from the neighbor.
Entry Last Changed Time	The time when the entry was last changed.

The following shows example CLI display output for the command.

```
(Switching) #show isdp entry Switch

Device ID Switch

Address(es):
IP Address:172.20.1.18
IP Address: 172.20.1.18
Capability Router IGMP

Platform cisco WS-C4948

Interface 0/1

Port ID GigabitEthernet1/1

Holdtime 64

Advertisement Version 2

Entry last changed time 0 days 00:13:50
```

show isdp neighbors

This command displays the list of neighboring devices.

Format	`show isdp neighbors [{slot/port | detail}]`
Mode	Privileged EXEC

Term	Definition
Device ID	The device ID associated with the neighbor which advertised the information.
IP Addresses	The IP addresses associated with the neighbor.
Capability	ISDP functional capabilities advertised by the neighbor.
Platform	The hardware platform advertised by the neighbor.
Interface	The interface (slot/port) on which the neighbor's advertisement was received.
Port ID	The port ID of the interface from which the neighbor sent the advertisement.
Hold Time	The hold time advertised by the neighbor.
Advertisement Version	The version of the advertisement packet received from the neighbor.
Entry Last Changed Time	Time when the entry was last modified.
Version	The software version that the neighbor is running.

The following shows example CLI display output for the command.

```
(CN1610) #show isdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route
Bridge,

                  S - Switch, H - Host, I - IGMP, r - Repeater

 Device ID          Intf Holdtime  Capability   Platform      Port
ID
------------------- ----- --------- ------------ ----------------
--- --------------------
```

```
Switch              0/1   165      RI              cisco WS-C4948
GigabitEthernet1/1
```

The following shows example CLI display output for the command.

```
(CN1610) #show isdp neighbors detail

Device ID 0001f45f1bc0
Address(es):
    IP Address: 10.27.7.57
Capability Router Trans Bridge Switch IGMP
Platform SecureStack C2
Interface 0/48
Port ID ge.3.14
Holdtime 131
Advertisement Version 2
Entry last changed time 0 days 00:01:59
Version:05.00.56
```

show isdp traffic

This command displays ISDP statistics.

Format	show isdp traffic
Mode	Privileged EXEC

Term	Definition
ISDP Packets Received	Total number of ISDP packets received
ISDP Packets Transmitted	Total number of ISDP packets transmitted
ISDPv1 Packets Received	Total number of ISDPv1 packets received
ISDPv1 Packets Transmitted	Total number of ISDPv1 packets transmitted
ISDPv2 Packets Received	Total number of ISDPv2 packets received
ISDPv2 Packets Transmitted	Total number of ISDPv2 packets transmitted

Term	Definition
ISDP Bad Header	Number of packets received with a bad header
ISDP Checksum Error	Number of packets received with a checksum error
ISDP Transmission Failure	Number of packets which failed to transmit
ISDP Invalid Format	Number of invalid packets received
ISDP Table Full	Number of times a neighbor entry was not added to the table due to a full database
ISDP IP Address Table Full	Displays the number of times a neighbor entry was added to the table without an IP address.

The following shows example CLI display output for the command.

```
(CN1610) #show isdp traffic

ISDP Packets Received..........................  4253
ISDP Packets Transmitted.......................  127
ISDPv1 Packets Received........................  0
ISDPv1 Packets Transmitted.....................  0
ISDPv2 Packets Received........................  4253
ISDPv2 Packets Transmitted.....................  4351
ISDP Bad Header................................  0
ISDP Checksum Error............................  0
ISDP Transmission Failure......................  0
ISDP Invalid Format............................  0
ISDP Table Full................................  392
ISDP IP Address Table Full.....................  737
```

debug isdp packet

This command enables tracing of ISDP packets processed by the switch. ISDP must be enabled on both the device and the interface in order to monitor packets for a particular interface.

Format	`debug isdp packet [{receive | transmit}]`
Mode	Privileged EXEC

no debug isdp packet

This command disables tracing of ISDP packets on the receive or the transmit sides or on both sides.

Format	`no debug isdp packet [{receive | transmit}]`
Mode	Privileged EXEC

IPv6 IPv6 Management Commands 6

This chapter describes the IPv6 commands available in the FASTPATH SMB CLI.

Note

The commands in this chapter are in one of three functional groups:

- Show commands display switch settings, statistics, and other information.
- Configuration commands configure features and options of the switch. For every configuration command, there is a show command that displays the configuration setting.
- Clear commands clear some or all of the settings to factory defaults.

IPv6 Management Commands

IPv6 Management commands allow a device to be managed via an IPv6 address in a switch or IPv4 routing (i.e., independent from the IPv6 Routing package). For Routing/IPv6 builds of FASTPATH dual IPv4/IPv6 operation over the service port is enabled. FASTPATH has capabilities such as:

- Static assignment of IPv6 addresses and gateways for the service/network ports.
- The ability to ping an IPv6 link-local address over the service/network port.
- Using IPv6 Management commands, you can send SNMP traps and queries via the service/network port.
- The user can manage a device via the network port (in addition to a Routing Interface or the Service port).

serviceport ipv6 enable

Use this command to enable IPv6 operation on the service port. By default, IPv6 operation is enabled on the service port.

Default	enabled
Format	`serviceport ipv6 enable`
Mode	Privileged EXEC

no serviceport ipv6 enable

Use this command to disable IPv6 operation on the service port.

Format	`no serviceport ipv6 enable`
Mode	Privileged EXEC

network ipv6 enable

Use this command to enable IPv6 operation on the network port. By default, IPv6 operation is enabled on the network port.

Default	enabled
Format	`network ipv6 enable`
Mode	Privileged EXEC

no network ipv6 enable

Use this command to disable IPv6 operation on the network port.

Format	`no network ipv6 enable`
Mode	Privileged EXEC

serviceport ipv6 address

Use the options of this command to manually configure IPv6 global address, enable/disable stateless global address autoconfiguration and to enable/disable dhcpv6 client protocol information on the service port.

Note
Multiple IPv6 prefixes can be configured on the service port.

Format	`serviceport ipv6 address {`*`address/prefix-length`* `[eui64]|autoconfig|dhcp}`
Mode	Privileged EXEC

Parameter	Description
address	IPv6 prefix in IPv6 global address format.
prefix-length	IPv6 prefix length value.
eui64	Formulate IPv6 address in eui64 address format.
autoconfig	Configure stateless global address autoconfiguration capability.
dhcp	Configure dhcpv6 client protocol.

no serviceport ipv6 address

Use the command `no serviceport ipv6 address` to remove all configured IPv6 prefixes on the service port interface.

Use the command with the address option to remove the manually configured IPv6 global address on the network port interface.

Use the command with the autoconfig option to disable the stateless global address autoconfiguration on the service port.

Use the command with the dhcp option to disable the dhcpv6 client protocol on the service port.

Format	`no serviceport ipv6 address {`*`address/prefix-length`* `[eui64] | autoconfig | dhcp}`
Mode	Privileged EXEC

serviceport ipv6 gateway

Use this command to configure IPv6 gateway (i.e. Default routers) information for the service port.

Note

Only a single IPv6 gateway address can be configured for the service port. There may be a combination of IPv6 prefixes and gateways that are explicitly configured and those that are set through auto-address configuration with a connected IPv6 router on their service port interface.

Format	`serviceport ipv6 gateway` *`gateway-address`*
Mode	Privileged EXEC

Parameter	Description
gateway-address	Gateway address in IPv6 global or link-local address format.

no serviceport ipv6 gateway

Use this command to remove IPv6 gateways on the service port interface.

Format	`no serviceport ipv6 gateway`
Mode	Privileged EXEC

serviceport ipv6 neighbor

Use this command to manually add IPv6 neighbors to the IPv6 neighbor table for the service port. If an IPv6 neighbor already exists in the neighbor table, the entry is automatically converted to a static entry. Static entries are not modified by the

neighbor discovery process. They are, however, treated the same for IPv6 forwarding. Static IPv6 neighbor entries are applied to the kernel stack and to the hardware when the corresponding interface is operationally active.

Format	`serviceport ipv6 neighbor` *`ipv6-address macaddr`*
Mode	Privileged EXEC

Parameter	Description
ipv6-address	The IPv6 address of the neighbor or interface.
macaddr	The link-layer address.

no serviceport ipv6 neighbor

Use this command to remove IPv6 neighbors from the IPv6 neighbor table for the service port.

Format	`no serviceport ipv6 neighbor` *`ipv6-address macaddr`*
Mode	Privileged EXEC

network ipv6 address

Use the options of this command to manually configure IPv6 global address, enable/disable stateless global address autoconfiguration and to enable/disable dhcpv6 client protocol information for the network port. Multiple IPv6 addresses can be configured on the network port.

Format	`network ipv6 address {`*`address/prefix-length`* `[eui64] | autoconfig | dhcp}`
Mode	Privileged EXEC

Parameter	Description
address	IPv6 prefix in IPv6 global address format.
prefix-length	IPv6 prefix length value.
eui64	Formulate IPv6 address in eui64 format.

Parameter	Description
autoconfig	Configure stateless global address autoconfiguration capability.
dhcp	Configure dhcpv6 client protocol.

no network ipv6 address

The command `no network ipv6 address` removes all configured IPv6 prefixes.

Use this command with the address option to remove the manually configured IPv6 global address on the network port interface.

Use this command with the autoconfig option to disable the stateless global address autoconfiguration on the network port.

Use this command with the dhcp option disables the dhcpv6 client protocol on the network port.

Format	`no network ipv6 address {`*`address/prefix-length`* `[eui64] | autoconfig | dhcp}`
Mode	Privileged EXEC

network ipv6 gateway

Use this command to configure IPv6 gateway (i.e. default routers) information for the network port.

Format	`network ipv6 gateway` *`gateway-address`*
Mode	Privileged EXEC

Parameter	Description
gateway-address	Gateway address in IPv6 global or link-local address format.

no network ipv6 gateway

Use this command to remove IPv6 gateways on the network port interface.

Format	`no network ipv6 gateway`
Mode	Privileged EXEC

network ipv6 neighbor

Use this command to manually add IPv6 neighbors to the IPv6 neighbor table for this network port. If an IPv6 neighbor already exists in the neighbor table, the entry is automatically converted to a static entry. Static entries are not modified by the neighbor discovery process. They are, however, treated the same for IPv6 forwarding. Static IPv6 neighbor entries are applied to the kernel stack and to the hardware when the corresponding interface is operationally active.

Format	`network ipv6 neighbor` *`ipv6-address macaddr`*
Mode	Privileged EXEC

Parameter	Description
ipv6-address	The IPv6 address of the neighbor or interface.
macaddr	The link-layer address.

no network ipv6 neighbor

Use this command to remove IPv6 neighbors from the neighbor table.

Format	`no network ipv6 neighbor` *`ipv6-address macaddr`*
Mode	Privileged EXEC

show network ipv6 neighbors

Use this command to display the information about the IPv6 neighbor entries cached on the network port. The information is updated to show the type of the entry.

Default	None
Format	`show network ipv6 neighbors`
Mode	◆ Privileged EXEC

Field	Description
IPv6 Address	The IPv6 address of the neighbor.
MAC Address	The MAC Address of the neighbor.
isRtr	Shows if the neighbor is a router. If TRUE, the neighbor is a router; FALSE it is not a router.
Neighbor State	The state of the neighbor cache entry. Possible values are: Incomplete, Reachable, Stale, Delay, Probe, and Unknown
Age	The time in seconds that has elapsed since an entry was added to the cache.
Last Updated	The time in seconds that has elapsed since an entry was added to the cache.
Type	The type of neighbor entry. The type is Static if the entry is manually configured and Dynamic if dynamically resolved.

The following is an example of the command.

```
(CN1610) #show network ipv6 neighbors

                                                    Neighbor  Age
IPv6 Address             MAC Address       isRtr State    (Secs)
     Type
------------------------ ----------------- ----- --------- ------
     ------
FE80::5E26:AFF:FEBD:852C 5c:26:0a:bd:85:2c FALSE Reachable 0
         Static
```

show serviceport ipv6 neighbors

Use this command to displays information about the IPv6 neighbor entries cached on the service port. The information is updated to show the type of the entry.

Default	None
Format	`show serviceport ipv6 neighbors`
Mode	Privileged EXEC

Field	Description
IPv6 Address	The IPv6 address of the neighbor.
MAC Address	The MAC Address of the neighbor.
isRtr	Shows if the neighbor is a router. If TRUE, the neighbor is a router; if FALSE, it is not a router.
Neighbor State	The state of the neighbor cache entry. The possible values are: Incomplete, Reachable, Stale, Delay, Probe, and Unknown.
Age	The time in seconds that has elapsed since an entry was added to the cache.
Type	The type of neighbor entry. The type is Static if the entry is manually configured and Dynamic if dynamically resolved.

The following is an example of the command.

```
(CN1610) #show serviceport ipv6 neighbors

                                                                  Neighbor
Age
IPv6 Address                          MAC Address      isRtr State
(Secs)   Type
------------------------------------- ----------------- ----- ---
------ ------  --------
FE80::5E26:AFF:FEBD:852C                5c:26:0a:bd:85:2c FALSE
Reachable 0       Dynamic
```

ping ipv6

Use this command to determine whether another computer is on the network. Ping provides a synchronous response when initiated from the CLI and Web interfaces. To use the command, configure the switch for network (in-band) connection. The source and target devices must have the ping utility enabled and running on top of TCP/IP. The switch can be pinged from any IP workstation with which the switch is connected through the default VLAN (VLAN 1), as long as there is a physical path between the switch and the workstation. The terminal interface sends three pings to the target station. Use the *ipv6-address|hostname* parameter to ping an interface by using the global IPv6 address of the interface. The argument slot/port corresponds to a physical routing

interface or VLAN routing interface. The keyword **vlan** is used to specify the VLAN ID of the routing VLAN directly instead of a slot/port format. Use the optional *size* keyword to specify the size of the ping packet.

You can utilize the ping or traceroute facilities over the service/network ports when using an IPv6 global address *ipv6-global-address|hostname*. Any IPv6 global address or gateway assignments to these interfaces will cause IPv6 routes to be installed within the IP stack such that the ping or traceroute request is routed out the service/network port properly. When referencing an IPv6 link-local address, you must also specify the service or network port interface by using the *serviceport* or *network* parameter.

Default	◆ The default count is 1. ◆ The default interval is 3 seconds. ◆ The default size is 0 bytes.
Format	ping ipv6 {*ipv6-global-address*|*hostname* | {interface {slot/port|*vlan 1-4093*| serviceport | network} *link-local-address*} [size *datagram-size]*}
Mode	◆ Privileged EXEC ◆ User EXEC

ping ipv6 interface

Use this command to determine whether another computer is on the network. To use the command, configure the switch for network (in-band) connection. The source and target devices must have the ping utility enabled and running on top of TCP/IP. The switch can be pinged from any IP workstation with which the switch is connected through the default VLAN (VLAN 1), as long as there is a physical path between the switch and the workstation. The terminal interface sends three pings to the target station. You can use a network port, service port, vlan, or physical interface as the source. The argument slot/port corresponds to a physical routing interface or VLAN routing interface. The keyword **vlan** is used to specify the VLAN ID of the routing VLAN directly instead of in a slot/port format.

Format	ping ipv6 interface {slot/port|vlan *1-4093* |network |serviceport} {link-local-address *link-local-address* | *ipv6-address*} [size *datagram-size*]
Modes	◆ Privileged EXEC ◆ User EXEC

Keyword	Description
interface	Use the *interface* keyword to ping an interface by using the link-local address or the global IPv6 address of the interface.
size	Use the optional *size* keyword to specify the size of the ping packet.
ipv6-address	The link local IPv6 address of the device you want to query.

Quality of Service Commands 7

This chapter describes the Quality of Service (QoS) commands available in the FASTPATH CLI.

The QoS Commands chapter contains the following sections:

Note

The commands in this chapter are in one of two functional groups:

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

Class of Service Commands

This section describes the commands you use to configure and view Class of Service (CoS) settings for the switch. The commands in this section allow you to control the priority and transmission rate of traffic.

Note
Commands you issue in the Interface Config mode only affect a single interface. Commands you issue in the Global Config mode affect all interfaces.

classofservice dot1p-mapping

This command maps an 802.1p priority to an internal traffic class. The *userpriority* values can range from 0-7. The *trafficclass* values range from 0-7.

Format	`classofservice dot1p-mapping` *`userpriority trafficclass`*
Modes	◆ Global Config ◆ Interface Config

no classofservice dot1p-mapping

This command maps each 802.1p priority to its default internal traffic class value.

Format	`no classofservice dot1p-mapping`
Modes	◆ Global Config ◆ Interface Config

classofservice ip-dscp-mapping

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

Format	`classofservice ip-dscp-mapping` *`ipdscp trafficclass`*
Mode	Global Config

no classofservice ip-dscp-mapping

This command maps each IP DSCP value to its default internal traffic class value.

Format	`no classofservice ip-dscp-mapping`
Mode	Global Config

classofservice trust

This command sets the class of service trust mode of an interface or range of interfaces. You can set the mode to trust one of the Dot1p (802.1p), IP DSCP, or IP Precedence packet markings. You can also set the interface mode to untrusted. If you configure an interface to use Dot1p, the mode does not appear in the output of the "show running-config" on page 177 command because Dot1p is the default.

Note

The `classofservice trust dot1p` command will not be supported in future releases of the software because Dot1p is the default value. Use the `no classofservice trust` command to set the mode to the default value.

Default	dot1p
Format	`classofservice trust {dot1p | ip-dscp | untrusted}`
Modes	◆ Global Config ◆ Interface Config

no classofservice trust

This command sets the interface mode to the default value.

Format	`no classofservice trust`
Modes	◆ Global Config ◆ Interface Config

cos-queue min-bandwidth

This command specifies the minimum transmission bandwidth guarantee for each interface queue on an interface, a range of interfaces, or all interfaces. A value from 0-100 (percentage of link rate) must be specified for each supported queue, with 0 indicating no guaranteed minimum bandwidth. The sum of all values entered must not exceed 100.

Format	`cos-queue min-bandwidth` *`bw-0 bw-1 … bw-n`*
Modes	◆ Global Config ◆ Interface Config

no cos-queue min-bandwidth

This command restores the default for each queue's minimum bandwidth value.

Format	`no cos-queue min-bandwidth`
Modes	◆ Global Config ◆ Interface Config

cos-queue random-detect

This command activates weighted random early discard (WRED) for each specified queue on the interface. Specific WRED parameters are configured using the `random-detect queue-parms` and the `random-detect exponential-weighting-constant` commands.

Format	`cos-queue random-detect` *`queue-id-1`* [*`queue-id-2 … queue-id-n`*]
Modes	◆ Global Config ◆ Interface Config

When specified in Interface Config' mode, this command affects a single interface only, whereas in Global Config mode, it applies to all interfaces.

At least one, but no more than *n* queue-id values are specified with this command. Duplicate queue-id values are ignored. Each queue-id value ranges from 0 to (*n*–1), where n is the total number of queues supported per interface. The number *n* = 7 and corresponds to the number of supported queues (traffic classes).

no cos-queue random-detect

Use this command to disable WRED, thereby restoring the default tail drop operation for the specified queues on the interface.

Format	`no cos-queue random-detect` *`queue-id-1`* [*`queue-id-2 … queue-id-n`*]

Modes	◆ Global Config ◆ Interface Config

cos-queue strict

This command activates the strict priority scheduler mode for each specified queue for an interface queue on an interface, a range of interfaces, or all interfaces.

Format	`cos-queue strict` *`queue-id-1 [queue-id-2 … queue-id-n]`*
Modes	◆ Global Config ◆ Interface Config

no cos-queue strict

This command restores the default weighted scheduler mode for each specified queue.

Format	`no cos-queue strict` *`queue-id-1`* [*`queue-id-2 … queue-id-n`*]
Modes	◆ Global Config ◆ Interface Config

random-detect

This command is used to enable WRED for the interface as a whole, and is only available when per-queue WRED activation control is not supported by the device Specific WRED parameters are configured using the `random-detect queue-parms` and the `random-detect exponential-weighting-constant` commands.

Format	`random-detect`
Modes	◆ Global Config ◆ Interface Config

When specified in Interface Config mode, this command affects a single interface only, whereas in Global Config mode, it applies to all interfaces.

no random-detect

Use this command to disable WRED, thereby restoring the default tail drop operation for all queues on the interface.

Format	`no random-detect`
Modes	◆ Global Config ◆ Interface Config

random-detect exponential weighting-constant

This command is used to configure the WRED decay exponent for a CoS queue interface.

Format	`random-detect exponential-weighting-constant` *`0-15`*
Modes	◆ Global Config ◆ Interface Config

no random-detect exponential-weighting-constant

Use this command to set the WRED decay exponent back to the default.

Format	`no random-detect exponential-weighting-constant`
Modes	◆ Global Config ◆ Interface Config

random-detect queue-parms

This command is used to configure WRED parameters for each drop precedence level supported by a queue. It is used only when per-COS queue configuration is enabled (using the `cos-queue random-detect` command).

Format	`random-detect queue-parms` *`queue-id-1`* `[`*`queue-id-2 … queue-id-n`*`] min-thresh` *`thresh-prec-1 … thresh-prec-n`* `max-thresh` *`thresh-prec-1 … thresh-prec-n`* `drop-probability` *`prob-prec-1 … prob-prec-n`*
Modes	◆ Global Config ◆ Interface Config

Each parameter is specified for each possible drop precedence (*color* of TCP traffic). The last precedence applies to all non-TCP traffic. For example, in a 3-color system, four of each parameter specified: green TCP, yellow TCP, red TCP, and non-TCP, respectively.

Term	Definition
min-thresh	The minimum threshold the queue depth (as a percentage) where WRED starts marking and dropping traffic.
max-thresh	The maximum threshold is the queue depth (as a percentage) above which WRED marks / drops all traffic.
drop-probability	The percentage probability that WRED will mark/drop a packet, when the queue depth is at the maximum threshold. (The drop probability increases linearly from 0 just before the minimum threshold, to this value at the maximum threshold, then goes to 100% for larger queue depths).

no random-detect queue-parms

Use this command to set the WRED configuration back to the default.

Format	`no random-detect queue-parms` *`queue-id-1`* [*`queue-id-2 … queue-id-n`*]
Modes	◆ Global Config ◆ Interface Config

traffic-shape

This command specifies the maximum transmission bandwidth limit for the interface as a whole. The bandwidth values are from 0-100 in increments of 1. You can also specify this value for a range of interfaces or all interfaces. Also known as rate shaping, traffic shaping has the effect of smoothing temporary traffic bursts over time so that the transmitted traffic rate is bounded.

Format	`traffic-shape` *`bw`*

Modes	◆ Global Config ◆ Interface Config

no traffic-shape

This command restores the interface shaping rate to the default value.

Format	`no traffic-shape`
Modes	◆ Global Config ◆ Interface Config

show classofservice dot1p-mapping

This command displays the current Dot1p (802.1p) priority mapping to internal traffic classes for a specific interface.

If specified, the 802.1p mapping table of the interface is displayed. If omitted, the most recent global configuration settings are displayed. For more information, see "Voice VLAN Commands" on page 382.

Format	`show classofservice dot1p-mapping [slot/port]`
Mode	Privileged EXEC

The following information is repeated for each user priority.

Term	Definition
User Priority	The 802.1p user priority value.
Traffic Class	The traffic class internal queue identifier to which the user priority value is mapped.

show classofservice ip-dscp-mapping

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

Format	`show classofservice ip-dscp-mapping`
Mode	Privileged EXEC

The following information is repeated for each user priority.

Term	Definition
IP DSCP	The IP DSCP value.
Traffic Class	The traffic class internal queue identifier to which the IP DSCP value is mapped.

show classofservice trust

This command displays the current trust mode setting for a specific interface. If you specify an interface, the command displays the port trust mode of the interface. If you do not specify an interface, the command displays the most recent global configuration settings.

Format	`show classofservice trust [slot/port]`
Mode	Privileged EXEC

Term	Definition
Class of Service Trust Mode	The the trust mode, which is either Dot1P, IP DSCP, or Untrusted.
Non-IP Traffic Class	(IP DSCP mode only) The traffic class used for non-IP traffic.
Untrusted Traffic Class	(Untrusted mode only) The traffic class used for all untrusted traffic.

show interfaces cos-queue

This command displays the class-of-service queue configuration for the specified interface. If specified, the class-of-service queue configuration of the interface is displayed. If omitted, the most recent global configuration settings are displayed.

Format	`show interfaces cos-queue [slot/port]`
Mode	Privileged EXEC

Term	Definition
Interface Shaping Rate	The global interface shaping rate value.
WRED Decay Exponent	The global WRED decay exponent value.
Queue Id	An interface supports n queues numbered 0 to (n-1).
Minimum Bandwidth	The minimum transmission bandwidth guarantee for the queue, expressed as a percentage. A value of 0 means bandwidth is not guaranteed and the queue operates using best-effort. This is a configured value.
Scheduler Type	Indicates whether this queue is scheduled for transmission using a strict priority or a weighted scheme. This is a configured value.
Queue Management Type	The queue depth management technique used for this queue (tail drop).

If you specify the interface, the command also displays the following information.

Term	Definition
Interface	The slot/port of the interface. If displaying the global configuration, this output line is replaced with a Global Config indication.
Interface Shaping Rate	The maximum transmission bandwidth limit for the interface as a whole. It is independent of any per-queue maximum bandwidth value(s) in effect for the interface. This is a configured value.
WRED Decay Exponent	The configured WRED decay exponent for a CoS queue interface.

show interfaces random-detect

This command displays the global WRED settings for each CoS queue. If you specify the slot/port, the command displays the WRED settings for each CoS queue on the specified interface.

Format	`show interfaces random-detect [slot/port]`
Mode	Privileged EXEC

Term	Definition
Queue ID	An interface supports n queues numbered 0 to (n-1).
WRED Minimum Threshold	The configured minimum threshold the queue depth (as a percentage) where WRED starts marking and dropping traffic.
WRED Maximum Threshold	The configured maximum threshold is the queue depth (as a percentage) above which WRED marks / drops all traffic.
WRED Drop Probability	The configured percentage probability that WRED will mark/drop a packet, when the queue depth is at the maximum threshold. (The drop probability increases linearly from 0 just before the minimum threshold, to this value at the maximum threshold, then goes to 100% for larger queue depths).

Differentiated Services Commands

This section describes the commands you use to configure QOS Differentiated Services (DiffServ).

You configure DiffServ in several stages by specifying three DiffServ components:

1. Class
   - ❖ Creating and deleting classes.
   - ❖ Defining match criteria for a class.
2. Policy
   - ❖ Creating and deleting policies
   - ❖ Associating classes with a policy
   - ❖ Defining policy statements for a policy/class combination
3. Service
   - ❖ Adding and removing a policy to/from an inbound interface

The DiffServ class defines the packet filtering criteria. The attributes of a DiffServ policy define the way the switch processes packets. You can define policy attributes on a per-class instance basis. The switch applies these attributes when a match occurs.

Packet processing begins when the switch tests the match criteria for a packet. The switch applies a policy to a packet when it finds a class match within that policy.

The following rules apply when you create a DiffServ class:

- ◆ Each class can contain a maximum of one referenced (nested) class
- ◆ Class definitions do not support hierarchical service policies

A given class definition can contain a maximum of one reference to another class. You can combine the reference with other match criteria. The referenced class is truly a reference and not a copy since additions to a referenced class affect all classes that reference it. Changes to any class definition currently referenced by any other class must result in valid class definitions for all derived classes, otherwise the switch rejects the change. You can remove a class reference from a class definition.

The only way to remove an individual match criterion from an existing class definition is to delete the class and re-create it.

Note

The mark possibilities for policing include CoS, IP DSCP, and IP Precedence. While the latter two are only meaningful for IP packet types, CoS marking is allowed for both IP and non-IP packets, since it updates the 802.1p user priority field contained in the VLAN tag of the layer 2 packet header.

diffserv

This command sets the DiffServ operational mode to active. While disabled, the DiffServ configuration is retained and can be changed, but it is not activated. When enabled, DiffServ services are activated.

Format	`diffserv`
Mode	Global Config

no diffserv

This command sets the DiffServ operational mode to inactive. While disabled, the DiffServ configuration is retained and can be changed, but it is not activated. When enabled, DiffServ services are activated.

Format	`no diffserv`
Mode	Global Config

DiffServ Class Commands

Use the DiffServ class commands to define traffic classification. To classify traffic, you specify Behavior Aggregate (BA), based on DSCP and Multi-Field (MF) classes of traffic (name, match criteria)

This set of commands consists of class creation/deletion and matching, with the class match commands specifying Layer 3, Layer 2, and general match criteria. The class match criteria are also known as class rules, with a class definition consisting of one or more rules to identify the traffic that belongs to the class.

Note
Once you create a class match criterion for a class, you cannot change or delete the criterion. To change or delete a class match criterion, you must delete and re-create the entire class.

The CLI command root is `class-map`.

class-map

This command defines a DiffServ class of type match-all. When used without any match condition, this command enters the class-map mode. The *`class-map-name`* is a case sensitive alphanumeric string from 1 to 31 characters uniquely identifying an existing DiffServ class.

Note
The class-map-name 'default' is reserved and must not be used.

The class type of `match-all` indicates all of the individual match conditions must be true for a packet to be considered a member of the class.This command may be used without specifying a class type to enter the Class-Map Config mode for an existing DiffServ class.

Note
The optional keywords [`{ipv4 | ipv6}`] specify the Layer 3 protocol for this class. If not specified, this parameter defaults to `ipv4`. This maintains backward compatibility for configurations defined on systems before IPv6 match items were supported.

Note

The CLI mode is changed to Class-Map Config or Ipv6-Class-Map Config when this command is successfully executed depending on the [{ipv4 | ipv6}] keyword specified.

Format	class-map match-all *class-map-name* [{ipv4 | ipv6}]
Mode	Global Config

no class-map

This command eliminates an existing DiffServ class. The *class-map-name* is the name of an existing DiffServ class. (The class name **default** is reserved and is not allowed here.) This command may be issued at any time; if the class is currently referenced by one or more policies or by any other class, the delete action fails.

Format	no class-map *class-map-name*
Mode	Global Config

class-map rename

This command changes the name of a DiffServ class. The *class-map-name* is the name of an existing DiffServ class. The *new-class-map-name* parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the class.

Default	none
Format	class-map rename *class-map-name new-class-map-name*
Mode	Global Config

match ethertype

This command adds to the specified class definition a match condition based on the value of the ethertype. The *ethertype* value is specified as one of the following keywords: appletalk, arp, ibmsna, ipv4, ipv6, ipx, mplsmcast, mplsucast, netbios, novell, pppoe, rarp or as a custom EtherType value in the range of 0x0600-0xFFFF. Use the [not] option to negate the match condition.

Format	`match [not] ethertype {keyword | custom 0x0600-0xFFFF}`
Mode	Class-Map Config Ipv6-Class-Map Config

match any

This command adds to the specified class definition a match condition whereby all packets are considered to belong to the class. Use the [not] option to negate the match condition.

Default	none
Format	`match [not] any`
Mode	Class-Map Config Ipv6-Class-Map Config

match class-map

This command adds to the specified class definition the set of match conditions defined for another class. The *refclassname* is the name of an existing DiffServ class whose match conditions are being referenced by the specified class definition.

Default	none
Format	`match class-map refclassname`
Mode	Class-Map Config Ipv6-Class-Map Config

Note

The match class-map command has the following criteria:

- The parameters *refclassname* and *class-map-name* can not be the same.
- Only one other class may be referenced by a class.
- Any attempts to delete the *refclassname* class while the class is still referenced by any *class-map-name* fails.
- The combined match criteria of *class-map-name* and *refclassname* must be an allowed combination based on the class type.

- Any subsequent changes to the *refclassname* class match criteria must maintain this validity, or the change attempt fails.
- The total number of class rules formed by the complete reference class chain (including both predecessor and successor classes) must not exceed a platform-specific maximum. In some cases, each removal of a refclass rule reduces the maximum number of available rules in the class definition by one.

---

no match class-map

This command removes from the specified class definition the set of match conditions defined for another class. The *refclassname* is the name of an existing DiffServ class whose match conditions are being referenced by the specified class definition.

Format	`no match class-map` *refclassname*
Mode	Class-Map Config Ipv6-Class-Map Config

match cos

This command adds to the specified class definition a match condition for the Class of Service value (the only tag in a single tagged packet or the first or outer 802.1Q tag of a double VLAN tagged packet). The value may be from 0 to 7. Use the [not] option to negate the match condition.

Default	none
Format	`match [not] cos` *0-7*
Mode	Class-Map Config Ipv6-Class-Map Config

match secondary-cos

This command adds to the specified class definition a match condition for the secondary Class of Service value (the inner 802.1Q tag of a double VLAN tagged packet). The value may be from 0 to 7. Use the [not] option to negate the match condition.

Default	none

Format	`match [not]secondary-cos 0-7`
Mode	Class-Map Config Ipv6-Class-Map Config

match destination-address mac

This command adds to the specified class definition a match condition based on the destination MAC address of a packet. The *macaddr* parameter is any layer 2 MAC address formatted as six, two-digit hexadecimal numbers separated by colons (e.g., 00:11:22:dd:ee:ff). The *macmask* parameter is a layer 2 MAC address bit mask, which need not be contiguous, and is formatted as six, two-digit hexadecimal numbers separated by colons (e.g., ff:07:23:ff:fe:dc). Use the [not] option to negate the match condition.

Default	none
Format	`match [not] destination-address mac macaddr macmask`
Mode	Class-Map Config Ipv6-Class-Map Config

match dstip

This command adds to the specified class definition a match condition based on the destination IP address of a packet. The *ipaddr* parameter specifies an IP address. The *ipmask* parameter specifies an IP address bit mask and must consist of a contiguous set of leading 1 bits. Use the [not] option to negate the match condition.

Default	none
Format	`match [not] dstip ipaddr ipmask`
Mode	Class-Map Config

match dstl4port

This command adds to the specified class definition a match condition based on the destination layer 4 port of a packet using a single keyword or numeric notation. To specify the match condition as a single keyword, the value for *portkey* is one of the supported port name keywords. The currently supported *portkey* values are: domain, echo, ftp, ftpdata, http, smtp, snmp, telnet, tftp,

www. Each of these translates into its equivalent port number. To specify the match condition using a numeric notation, one layer 4 port number is required. The port number is an integer from 0 to 65535. Use the [not] option to negate the match condition.

Default	none
Format	`match [not] dstl4port {portkey | 0-65535}`
Mode	Class-Map Config Ipv6-Class-Map Config

match ip dscp

This command adds to the specified class definition a match condition based on the value of the IP DiffServ Code Point (DSCP) field in a packet, which is defined as the high-order six bits of the Service Type octet in the IP header (the low-order two bits are not checked).

The *dscpval* value is specified as either an integer from 0 to 63, or symbolically through one of the following keywords: af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, ef. Use the [not] option to negate the match condition.

Note

The IP DSCP, IP Precedence, and IP ToS match conditions are alternative ways to specify a match criterion for the same Service Type field in the IP header, but with a slightly different user notation.

Default	none
Format	`match [not] ip dscp dscpval`
Mode	Class-Map Config Ipv6-Class-Map Config

match ip precedence

This command adds to the specified class definition a match condition based on the value of the IP Precedence field in a packet, which is defined as the high-order three bits of the Service Type octet in the IP header (the low-order five bits are not checked). The precedence value is an integer from 0 to 7. Use the [not] option to negate the match condition.

Note

The IP DSCP, IP Precedence, and IP ToS match conditions are alternative ways to specify a match criterion for the same Service Type field in the IP header, but with a slightly different user notation.

Default	none
Format	`match [not] ip precedence 0-7`
Mode	Class-Map Config

match ip tos

This command adds to the specified class definition a match condition based on the value of the IP TOS field in a packet, which is defined as all eight bits of the Service Type octet in the IP header. The value of *tosbits* is a two-digit hexadecimal number from 00 to ff. The value of *tosmask* is a two-digit hexadecimal number from 00 to ff. The *tosmask* denotes the bit positions in *tosbits* that are used for comparison against the IP TOS field in a packet. For example, to check for an IP TOS value having bits 7 and 5 set and bit 1 clear, where bit 7 is most significant, use a *tosbits* value of a0 (hex) and a *tosmask* of a2 (hex). Use the [not] option to negate the match condition.

Note

The IP DSCP, IP Precedence, and IP ToS match conditions are alternative ways to specify a match criterion for the same Service Type field in the IP header, but with a slightly different user notation.

Note

This “free form” version of the IP DSCP/Precedence/TOS match specification gives the user complete control when specifying which bits of the IP Service Type field are checked.

Default	none
Format	`match [not] ip tos tosbits tosmask`
Mode	Class-Map Config

match protocol

This command adds to the specified class definition a match condition based on the value of the IP Protocol field in a packet using a single keyword notation or a numeric value notation.

To specify the match condition using a single keyword notation, the value for `protocol-name` is one of the supported protocol name keywords. The currently supported values are: *icmp*, *igmp*, *ip*, *tcp*, *udp*. A value of *ip* matches all protocol number values.

To specify the match condition using a numeric value notation, the protocol number is a standard value assigned by IANA and is interpreted as an integer from 0 to 255. Use the [not] option to negate the match condition.

Note

This command does not validate the protocol number value against the current list defined by IANA.

Default	none
Format	`match [not] protocol {`*protocol-name	0-255*`}`
Mode	Class-Map Config Ipv6-Class-Map Config

match source-address mac

This command adds to the specified class definition a match condition based on the source MAC address of a packet. The *address* parameter is any layer 2 MAC address formatted as six, two-digit hexadecimal numbers separated by colons (e.g., 00:11:22:dd:ee:ff). The *macmask* parameter is a layer 2 MAC address bit mask, which may not be contiguous, and is formatted as six, two-digit hexadecimal numbers separated by colons (e.g., ff:07:23:ff:fe:dc). Use the [not] option to negate the match condition.

Default	none
Format	`match [not] source-address mac` *address macmask*
Mode	Class-Map Config Ipv6-Class-Map Config

match srcip

This command adds to the specified class definition a match condition based on the source IP address of a packet. The *ipaddr* parameter specifies an IP address. The *ipmask* parameter specifies an IP address bit mask and must consist of a contiguous set of leading 1 bits. Use the [not] option to negate the match condition.

Default	none
Format	`match [not] srcip ipaddr ipmask`
Mode	Class-Map Config

match srcl4port

This command adds to the specified class definition a match condition based on the source layer 4 port of a packet using a single keyword or numeric notation. To specify the match condition as a single keyword notation, the value for *portkey* is one of the supported port name keywords (listed below). The currently supported *portkey* values are: domain, echo, ftp, ftpdata, http, smtp, snmp, telnet, tftp, www. Each of these translates into its equivalent port number, which is used as both the start and end of a port range.

To specify the match condition as a numeric value, one layer 4 port number is required. The port number is an integer from 0 to 65535. Use the [not] option to negate the match condition.

Default	none
Format	`match [not] srcl4port {portkey | 0-65535}`
Mode	Class-Map Config Ipv6-Class-Map Config

match vlan

This command adds to the specified class definition a match condition based on the value of the layer 2 VLAN Identifier field (the only tag in a single tagged packet or the first or outer tag of a double VLAN tagged packet). The VLAN ID is an integer from 0 to 4093. Use the [not] option to negate the match condition.

Default	none
Format	`match [not] vlan 0-4093`

Mode	Class-Map Config Ipv6-Class-Map Config

match secondary-vlan

This command adds to the specified class definition a match condition based on the value of the layer 2 secondary VLAN Identifier field (the inner 802.1Q tag of a double VLAN tagged packet). The secondary VLAN ID is an integer from 0 to 4093. Use the [not] option to negate the match condition.

Default	none
Format	`match [not] secondary-vlan` *`0-4093`*
Mode	Class-Map Config Ipv6-Class-Map Config

DiffServ Policy Commands

Use the DiffServ policy commands to specify traffic conditioning actions, such as policing and marking, to apply to traffic classes

Use the policy commands to associate a traffic class that you define by using the class command set with one or more QoS policy attributes. Assign the class/policy association to an interface to form a service. Specify the policy name when you create the policy.

Each traffic class defines a particular treatment for packets that match the class definition. You can associate multiple traffic classes with a single policy. When a packet satisfies the conditions of more than one class, preference is based on the order in which you add the classes to the policy. The first class you add has the highest precedence.

This set of commands consists of policy creation/deletion, class addition/removal, and individual policy attributes.

Note

The only way to remove an individual policy attribute from a class instance within a policy is to remove the class instance and re-add it to the policy. The values associated with an existing policy attribute can be changed without removing the class instance.

The CLI command root is `policy-map`.

assign-queue

This command modifies the queue id to which the associated traffic stream is assigned. The *queueid* is an integer from 0 to *n*-1, where *n* is the number of egress queues supported by the device.

Format	`assign-queue` *queueid*
Mode	Policy-Class-Map Config
Incompatibilities	Drop

drop

This command specifies that all packets for the associated traffic stream are to be dropped at ingress.

Format	`drop`
Mode	Policy-Class-Map Config
Incompatibilities	Assign Queue, Mark (all forms), Mirror, Police, Redirect

mirror

This command specifies that all incoming packets for the associated traffic stream are copied to a specific egress interface (physical port or LAG).

Format	`mirror slot/port`
Mode	Policy-Class-Map Config
Incompatibilities	Drop, Redirect

redirect

This command specifies that all incoming packets for the associated traffic stream are redirected to a specific egress interface (physical port or port-channel).

Format	`redirect slot/port`
Mode	Policy-Class-Map Config
Incompatibilities	Drop, Mirror

conform-color

Use this command to enable color-aware traffic policing and define the conform-color class map. Used in conjunction with the police command where the fields for the conform level are specified. The *`class-map-name`* parameter is the name of an existing DiffServ class map.

Note
This command may only be used after specifying a police command for the policy-class instance.

Format	`conform-color` *`class-map-name`*
Mode	Policy-Class-Map Config

class

This command creates an instance of a class definition within the specified policy for the purpose of defining treatment of the traffic class through subsequent policy attribute statements. The *`classname`* is the name of an existing DiffServ class.

Note
This command causes the specified policy to create a reference to the class definition.

Note
The CLI mode is changed to Policy-Class-Map Config when this command is successfully executed.

Format	`class` *`classname`*
Mode	Policy-Map Config

no class

This command deletes the instance of a particular class and its defined treatment from the specified policy. *`classname`* is the names of an existing DiffServ class.

Note
This command removes the reference to the class definition for the specified policy.

Format	`no class` *`classname`*
Mode	Policy-Map Config

mark cos

This command marks all packets for the associated traffic stream with the specified class of service (CoS) value in the priority field of the 802.1p header (the only tag in a single tagged packet or the first or outer 802.1Q tag of a double VLAN tagged packet). If the packet does not already contain this header, one is inserted. The CoS value is an integer from 0 to 7.

Default	1
Format	`mark-cos` *`0-7`*
Mode	Policy-Class-Map Config
Incompatibilities	Drop, Mark IP DSCP, IP Precedence, Police

mark cos-as-sec-cos

This command marks outer VLAN tag priority bits of all packets as the inner VLAN tag priority, marking Cos as Secondary CoS. This essentially means that the inner VLAN tag CoS is copied to the outer VLAN tag CoS.

Format	mark-cos-as-sec-cos
Mode	Policy-Class-Map Config
Incompatibilities	Drop, Mark IP DSCP, IP Precedence, Police

The following shows an example of the command.

```
(CN1610) (Config-policy-classmap)#mark cos-as-sec-cos
```

mark ip-dscp

This command marks all packets for the associated traffic stream with the specified IP DSCP value.

The *`dscpval`* value is specified as either an integer from 0 to 63, or symbolically through one of the following keywords: af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, ef.

Format	`mark ip-dscp` *`dscpval`*

Mode	Policy-Class-Map Config
Incompatibilities	Drop, Mark CoS, Mark IP Precedence, Police

mark ip-precedence

This command marks all packets for the associated traffic stream with the specified IP Precedence value. The IP Precedence value is an integer from 0 to 7.

Note

This command may not be used on IPv6 classes. IPv6 does not have a precedence field.

Format	`mark ip-precedence` *`0-7`*
Mode	Policy-Class-Map Config
Incompatibilities	Drop, Mark CoS, Mark IP Precedence, Police
Policy Type	In

police-simple

This command is used to establish the traffic policing style for the specified class. The simple form of the **police** command uses a single data rate and burst size, resulting in two outcomes: conform and violate. The conforming data rate is specified in kilobits-per-second (Kbps) and is an integer from 1 to 4294967295. The conforming burst size is specified in kilobytes (KB) and is an integer from 1 to 128.

For each outcome, the only possible actions are drop, set-cos-as-sec-cos, set-cos-transmit, set-sec-cos-transmit, set-dscp-transmit, set-prec-transmit, or transmit. In this simple form of the **police** command, the conform action defaults to transmit and the violate action defaults to drop. These actions can be set with this command once the style has been configured.

For set-dscp-transmit, a *dscpval* value is required and is specified as either an integer from 0 to 63, or symbolically through one of the following keywords: af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, ef.

For set-prec-transmit, an IP Precedence value is required and is specified as an integer from 0-7.

For set-cos-transmit an 802.1p priority value is required and is specified as an integer from 0-7.

Format	police-simple {*1-4294967295 1-128* conform-action {drop | set-cos-as-sec-cos | set-cos-transmit *0-7* | set-sec-cos-transmit *0-7* | set-prec-transmit *0-7* | set-dscp-transmit *0-63* | transmit} [violate-action {drop | set-cos-as-sec-cos | set-cos-transmit *0-7* | set-sec-cos-transmit *0-7* | set-prec-transmit *0-7* | set-dscp-transmit *0-63* | transmit}]}
Mode	Policy-Class-Map Config
Incompatibilities	Drop, Mark (all forms)

The following shows an example of the command.

```
(CN1610) (Config-policy-classmap)#police-simple 1 128 conform-
action transmit violate-action drop
```

police-single-rate

This command is the single-rate form of the **police** command and is used to establish the traffic policing style for the specified class. For each outcome, the only possible actions are drop, set-cos-as-sec-cost, set-cos-transmit, set-sec-cos-transmit, set-dscp-transmit, set-prec-transmit, or transmit. In this single-rate form of the **police** command, the conform action defaults to send, the exceed action defaults to drop, and the violate action defaults to drop. These actions can be set with this command once the style has been configured.

Format	police-single-rate {*1-4294967295 1-128 1-128* conform-action {drop | set-cos-as-sec-cos | set-cos-transmit *0-7* | set-sec-cos-transmit *0-7* | set-prec-transmit *0-7* | set-dscp-transmit *0-63* | transmit} exceed-action {drop | set-cos-as-sec-cos | set-cos-transmit *0-7* | set-sec-cos-transmit *0-7* | set-prec-transmit *0-7* | set-dscp-transmit *0-63* | transmit} [violate-action {drop | set-cos-as-sec-cos-transmit | set-cos-transmit *0-7* | set-sec-cos-transmit *0-7* | set-prec-transmit *0-7* | set-dscp-transmit *0-63* | transmit}]}
Mode	Policy-Class-Map Config

police-two-rate

This command is the two-rate form of the **police** command and is used to establish the traffic policing style for the specified class. For each outcome, the only possible actions are drop, set-cos-as-sec-cos, set-cos-transmit, set-sec-cos-transmit, set-dscp-transmit, set-prec-transmit, or transmit. In this two-rate form of the **police** command, the conform action defaults to send, the exceed action defaults to drop, and the violate action defaults to drop. These actions can be set with this command once the style has been configured.

Format	police-two-rate {*1-4294967295 1-4294967295 1-128 1-128* conform-action {drop | set-cos-as-sec-cos | set-cos-transmit *0-7* | set-sec-cos-transmit *0-7* | set-prec-transmit *0-7* | set-dscp-transmit *0-63* | transmit} exceed-action {drop | set-cos-as-sec-cos | set-cos-transmit *0-7* | set-sec-cos-transmit *0-7* | set-prec-transmit *0-7* | set-dscp-transmit *0-63* | transmit} [violate-action {drop | set-cos-as-sec-cos | set-cos-transmit *0-7* | set-sec-cos-transmit *0-7* | set-prec-transmit *0-7* | set-dscp-transmit *0-63* | transmit}]}
Mode	Policy-Class-Map Config

policy-map

This command establishes a new DiffServ policy. The *policyname* parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the policy. The type of policy is specific to the inbound traffic direction as indicated by the `in` parameter, or the outbound traffic direction as indicated by the `out` parameter, respectively.

Note

The CLI mode is changed to Policy-Map Config when this command is successfully executed.

Format	`policy-map` *`policyname`* `{in|out}`
Mode	Global Config

no policy-map

This command eliminates an existing DiffServ policy. The *`policyname`* parameter is the name of an existing DiffServ policy. This command may be issued at any time. If the policy is currently referenced by one or more interface service attachments, this delete attempt fails.

Format	`no policy-map` *`policyname`*
Mode	Global Config

policy-map rename

This command changes the name of a DiffServ policy. The *`policyname i`*s the name of an existing DiffServ class. The *`newpolicyname`* parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the policy.

Format	`policy-map rename` *`policyname newpolicyname`*
Mode	Global Config

DiffServ Service Commands

Use the DiffServ service commands to assign a DiffServ traffic conditioning policy, which you specified by using the policy commands, to an interface in the incoming direction

The service commands attach a defined policy to a directional interface. You can assign only one policy at any one time to an interface in the inbound direction. DiffServ is not used in the outbound direction.

This set of commands consists of service addition/removal.

The CLI command root is `service-policy`.

service-policy

This command attaches a policy to an interface in the inbound direction as indicated by the `in` parameter, or the outbound direction as indicated by the `out` parameter, respectively. The *`policyname`* parameter is the name of an existing DiffServ policy. This command causes a service to create a reference to the policy.

Note
This command effectively enables DiffServ on an interface in the inbound direction. There is no separate interface administrative 'mode' command for DiffServ.

Note
This command fails if any attributes within the policy definition exceed the capabilities of the interface. Once a policy is successfully attached to an interface, any attempt to change the policy definition, that would result in a violation of the interface capabilities, causes the policy change attempt to fail.

Note
Each interface can have one policy attached.

Format	`service-policy {in|out} policymapname`
Modes	◆ Global Config ◆ Interface Config

no service-policy

This command detaches a policy from an interface in the inbound direction as indicated by the `in` parameter, or the outbound direction as indicated by the `out` parameter, respectively. The *`policyname`* parameter is the name of an existing DiffServ policy.

Note

This command causes a service to remove its reference to the policy. This command effectively disables DiffServ on an interface in the inbound direction or an interface in the outbound direction. There is no separate interface administrative 'mode' command for DiffServ.

Format	`no service-policy {in|out} policymapname`
Modes	◆ Global Config ◆ Interface Config

DiffServ Show Commands

Use the DiffServ show commands to display configuration and status information for classes, policies, and services. You can display DiffServ information in summary or detailed formats. The status information is only shown when the DiffServ administrative mode is enabled.

show class-map

This command displays all configuration information for the specified class. The *class-name* is the name of an existing DiffServ class.

Format	`show class-map` *class-name*
Modes	◆ Privileged EXEC ◆ User EXEC

If the class-name is specified the following fields are displayed:

Term	Definition
Class Name	The name of this class.
Class Type	A class type of all means every match criterion defined for the class is evaluated simultaneously and must all be true to indicate a class match.
Class Layer3 Protocol	The Layer 3 protocol for this class. Possible values are IPv4 and IPv6.
Match Criteria	The Match Criteria fields are only displayed if they have been configured. Match criteria values are displayed in the order entered by the user. The fields are evaluated in accordance with the class type. The possible Match Criteria fields are: Destination IP Address, Destination Layer 4 Port, Destination MAC Address, Ethertype, Source MAC Address, VLAN, Class of Service, Every, IP DSCP, IP Precedence, IP TOS, Protocol Keyword, Reference Class, Source IP Address, and Source Layer 4 Port.
Values	The values of the Match Criteria.

If you do not specify the Class Name, this command displays a list of all defined DiffServ classes. The following fields are displayed:

Term	Definition
Class Name	The name of this class. (Note that the order in which classes are displayed is not necessarily the same order in which they were created.)
Class Type	A class type of all means every match criterion defined for the class is evaluated simultaneously and must all be true to indicate a class match.
Ref Class Name	The name of an existing DiffServ class whose match conditions are being referenced by the specified class definition.

show diffserv

This command displays the DiffServ General Status Group information, which includes the current administrative mode setting as well as the current and maximum number of rows in each of the main DiffServ private MIB tables. This command takes no options.

Format	`show diffserv`
Mode	Privileged EXEC

Term	Definition
DiffServ Admin mode	The current value of the DiffServ administrative mode.
Class Table Size Current/Max	The current and maximum number of entries (rows) in the Class Table.
Class Rule Table Size Current/Max	The current and maximum number of entries (rows) in the Class Rule Table.
Policy Table Size Current/Max	The current and maximum number of entries (rows) in the Policy Table.

Term	Definition
Policy Instance Table Size Current/Max	The current and maximum number of entries (rows) in the Policy Instance Table.
Policy Instance Table Max Current/Max	The current and maximum number of entries (rows) for the Policy Instance Table.
Policy Attribute Table Max Current/Max	The current and maximum number of entries (rows) for the Policy Attribute Table.
Service Table Size Current/Max	The current and maximum number of entries (rows) in the Service Table.

show policy-map

This command displays all configuration information for the specified policy. The *policyname* is the name of an existing DiffServ policy.

Format	`show policy-map` *[policyname]*
Mode	Privileged EXEC

If the Policy Name is specified the following fields are displayed:

Term	Definition
Policy Name	The name of this policy.
Policy Type	The policy type (only inbound policy definitions are supported for this platform.)
Class Members	The class that is a member of the policy.

The following information is repeated for each class associated with this policy (only those policy attributes actually configured are displayed):

Term	Definition
Assign Queue	Directs traffic stream to the specified QoS queue. This allows a traffic classifier to specify which one of the supported hardware queues are used for handling packets belonging to the class.

Term	Definition
Class Name	The name of this class.
Committed Burst Size (KB)	The committed burst size, used in simple policing.
Committed Rate (Kbps)	The committed rate, used in simple policing.
Conform Action	The current setting for the action taken on a packet considered to conform to the policing parameters. This is not displayed if policing is not in use for the class under this policy.
Conform Color Mode	The current setting for the color mode. Policing uses either color blind or color aware mode. Color blind mode ignores the coloration (marking) of the incoming packet. Color aware mode takes into consideration the current packet marking when determining the policing outcome.
Conform COS	The CoS mark value if the conform action is set-cos-transmit.
Conform DSCP Value	The DSCP mark value if the conform action is set-dscp-transmit.
Conform IP Precedence Value	The IP Precedence mark value if the conform action is set-prec-transmit.
Drop	Drop a packet upon arrival. This is useful for emulating access control list operation using DiffServ, especially when DiffServ and ACL cannot co-exist on the same interface.
Exceed Action	The action taken on traffic that exceeds settings that the network administrator specifies.
Exceed Color Mode	The current setting for the color of exceeding traffic that the user may optionally specify.

Term	Definition
Mark CoS	The class of service value that is set in the 802.1p header of inbound packets. This is not displayed if the mark cos was not specified.
Mark CoS as Secondary CoS	The secondary 802.1p priority value (second/inner VLAN tag. Same as CoS (802.1p) marking, but the dot1p value used for remarking is picked from the dot1p value in the secondary (i.e. inner) tag of a double-tagged packet.
Mark IP DSCP	The mark/re-mark value used as the DSCP for traffic matching this class. This is not displayed if mark ip description is not specified.
Mark IP Precedence	The mark/re-mark value used as the IP Precedence for traffic matching this class. This is not displayed if mark ip precedence is not specified.
Mirror	Copies a classified traffic stream to a specified egress port (physical port or LAG). This can occur in addition to any marking or policing action. It may also be specified along with a QoS queue assignment.
Non-Conform Action	The current setting for the action taken on a packet considered to not conform to the policing parameters. This is not displayed if policing not in use for the class under this policy.
Non-Conform COS	The CoS mark value if the non-conform action is set-cos-transmit.
Non-Conform DSCP Value	The DSCP mark value if the non-conform action is set-dscp-transmit.
Non-Conform IP Precedence Value	The IP Precedence mark value if the non-conform action is set-prec-transmit.

Term	Definition
Peak Rate	Guarantees a committed rate for transmission, but also transmits excess traffic bursts up to a user-specified peak rate, with the understanding that a downstream network element (such as the next hop's policer) might drop this excess traffic. Traffic is held in queue until it is transmitted or dropped (per type of queue depth management.) Peak rate shaping can be configured for the outgoing transmission stream for an AP traffic class (although average rate shaping could also be used.)
Peak Burst Size	(PBS). The network administrator can set the PBS as a means to limit the damage expedited forwarding traffic could inflict on other traffic (e.g., a token bucket rate limiter) Traffic that exceeds this limit is discarded.
Policing Style	The style of policing, if any, used (simple).
Redirect	Forces a classified traffic stream to a specified egress port (physical port or LAG). This can occur in addition to any marking or policing action. It may also be specified along with a QoS queue assignment.

If the Policy Name is not specified this command displays a list of all defined DiffServ policies. The following fields are displayed:

Term	Definition
Policy Name	The name of this policy. (The order in which the policies are displayed is not necessarily the same order in which they were created.)
Policy Type	The policy type (Only inbound is supported).
Class Members	List of all class names associated with this policy.

The following shows example CLI display output including the mark-cos-as-sec-cos option specified in the policy action.

```
(CN1610) #show policy-map p1
Policy Name..................................... p1
Policy Type..................................... In
Class Name...................................... c1
Mark CoS as Secondary CoS...................... Yes
```

The following shows example CLI display output including the mark-cos-as-sec-cos action used in the policing (simple-police, police-single-rate, police two-rate) command.

```
(CN1610) #show policy-map p2
Policy Name..................... p2
Policy Type..................... In
Class Name...................... c2
Policing Style.................. Police Two Rate
Committed Rate.................. 1
Committed Burst Size............ 1
Peak Rate....................... 1
Peak Burst Size................. 1
Conform Action.................. Mark CoS as Secondary CoS
Exceed Action................... Mark CoS as Secondary CoS
Non-Conform Action.............. Mark CoS as Secondary CoS
Conform Color Mode.............. Blind
Exceed Color Mode............... Blind
```

show diffserv service

This command displays policy service information for the specified interface and direction. The slot/port parameter specifies a valid slot/port number for the system.

Format	`show diffserv service slot/port in`
Mode	Privileged EXEC

Term	Definition
DiffServ Admin Mode	The current setting of the DiffServ administrative mode. An attached policy is only in effect on an interface while DiffServ is in an enabled mode.
Interface	slot/port
Direction	The traffic direction of this interface service.

Term	Definition
Operational Status	The current operational status of this DiffServ service interface.
Policy Name	The name of the policy attached to the interface in the indicated direction.
Policy Details	Attached policy details, whose content is identical to that described for the show policy-map *policymapname* command (content not repeated here for brevity).

show diffserv service brief

This command displays all interfaces in the system to which a DiffServ policy has been attached. The inbound direction parameter is optional.

Format	`show diffserv service brief [in]`
Mode	Privileged EXEC

Term	Definition
DiffServ Mode	The current setting of the DiffServ administrative mode. An attached policy is only active on an interface while DiffServ is in an enabled mode.

The following information is repeated for interface and direction (only those interfaces configured with an attached policy are shown):

Term	Definition
Interface	slot/port
Direction	The traffic direction of this interface service.
OperStatus	The current operational status of this DiffServ service interface.
Policy Name	The name of the policy attached to the interface in the indicated direction.

show policy-map interface

This command displays policy-oriented statistics information for the specified interface and direction. The slot/port parameter specifies a valid interface for the system. Instead of slot/port, `lag` *`lag-intf-num`* can be used as an alternate way to specify the LAG interface. `lag` *`lag-intf-num`* can also be used to specify the LAG interface where *`lag-intf-num`* is the LAG port number.

Note
This command is only allowed while the DiffServ administrative mode is enabled.

Format	`show policy-map interface slot/port [in]`
Mode	Privileged EXEC

Term	Definition
Interface	slot/port
Direction	The traffic direction of this interface service.
Operational Status	The current operational status of this DiffServ service interface.
Policy Name	The name of the policy attached to the interface in the indicated direction.

The following information is repeated for each class instance within this policy:

Term	Definition
Class Name	The name of this class instance.
In Discarded Packets	A count of the packets discarded for this class instance for any reason due to DiffServ treatment of the traffic class.

show service-policy

This command displays a summary of policy-oriented statistics information for all interfaces in the specified direction.

Format	`show service-policy in`

Mode	Privileged EXEC

The following information is repeated for each interface and direction (only those interfaces configured with an attached policy are shown):

Term	Definition
Interface	slot/port
Operational Status	The current operational status of this DiffServ service interface.
Policy Name	The name of the policy attached to the interface.

MAC Access Control List Commands

This section describes the commands you use to configure MAC Access Control List (ACL) settings. MAC ACLs ensure that only authorized users have access to specific resources and block any unwarranted attempts to reach network resources.

The following rules apply to MAC ACLs:

- The maximum number of ACLs you can create is hardware dependent. The limit applies to all ACLs, regardless of type.
- The system supports only Ethernet II frame types.
- The maximum number of rules per MAC ACL is hardware dependent.

mac access-list extended

This command creates a MAC Access Control List (ACL) identified by *name*, consisting of classification fields defined for the Layer 2 header of an Ethernet frame. The *name* parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the MAC access list. The rate-limit attribute configures the committed rate and the committed burst size.

If a MAC ACL by this name already exists, this command enters Mac-Access-List config mode to allow updating the existing MAC ACL.

Note
The CLI mode changes to Mac-Access-List Config mode when you successfully execute this command.

Format	`mac access-list extended` *name*
Mode	Global Config

no mac access-list extended

This command deletes a MAC ACL identified by *name* from the system.

Format	`no mac access-list extended` *name*
Mode	Global Config

mac access-list extended rename

This command changes the name of a MAC Access Control List (ACL). The *name* parameter is the name of an existing MAC ACL. The *newname* parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the MAC access list.

This command fails if a MAC ACL by the name *newname* already exists.

Format	`mac access-list extended rename name newname`
Mode	Global Config

{deny | permit} (MAC ACL)

This command creates a new rule for the current MAC access list. Each rule is appended to the list of configured rules for the list. A rule may either deny or permit traffic according to the specified classification fields. At a minimum, the source and destination MAC value must be specified, each of which may be substituted using the keyword any to indicate a match on any value in that field. The remaining command parameters are all optional, but the most frequently used parameters appear in the same relative order as shown in the command format.

Format	{deny|permit} {*srcmac* | any} {*dstmac* | any} [*ethertypekey* | *0x0600-0xFFFF*] [vlan {eq *0-4095*}] [cos *0-7*] [[log] [time-range *time-range-name*] [assign-queue *queue-id*]] [{mirror | redirect} slot/port][rate-limit *rate burst-size*]
Mode	Mac-Access-List Config

Note

The **no** form of this command is not supported, since the rules within a MAC ACL cannot be deleted individually. Rather, the entire MAC ACL must be deleted and respecified.

Note

An implicit **deny all** MAC rule always terminates the access list.

The Ethertype may be specified as either a keyword or a four-digit hexadecimal value from 0x0600-0xFFFF. The currently supported *ethertypekey* values are: appletalk, arp, ibmsna, ipv4, ipv6, ipx, mplsmcast, mplsucast, netbios, novell, pppoe, rarp. Each of these translates into its equivalent Ethertype value(s).

Ethertype Keyword	Corresponding Value
appletalk	0x809B
arp	0x0806
ibmsna	0x80D5
ipv4	0x0800
ipv6	0x86DD
ipx	0x8037
mplsmcast	0x8848
mplsucast	0x8847
netbios	0x8191
novell	0x8137, 0x8138
pppoe	0x8863, 0x8864
rarp	0x8035

The `vlan` and `cos` parameters refer to the VLAN identifier and 802.1p user priority fields, respectively, of the VLAN tag. For packets containing a double VLAN tag, this is the first (or outer) tag.

The `time-range` parameter allows imposing time limitation on the MAC ACL rule as defined by the parameter *time-range-name*. If a time range with the specified name does not exist and the MAC ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied immediately. If a time range with specified name exists and the MAC ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied when the time-range with specified name becomes active. The ACL rule is removed when the time-range with specified name becomes inactive. For information about configuring time ranges, see “Time Range Commands for Time-Based ACLs” on page 687.

The `assign-queue` parameter allows specification of a particular hardware queue for handling traffic that matches this rule. The allowed *`queue-id`* value is 0-(n-1), where n is the number of user configurable queues available for the hardware platform. The *`assign-queue`* parameter is valid only for a `permit` rule.

The *`assign-queue`* and *`redirect`* parameters are only valid for a `permit` rule.

Note

The special command form `{deny | permit} any any` is used to match all Ethernet layer 2 packets, and is the equivalent of the IP access list “match every” rule.

The **permit** command’s optional attribute **rate-limit** allows you to permit only the allowed rate of traffic as per the configured rate in kbps, and burst-size in kbytes.

The following shows an example of the command.

```
(CN1610) (Config)#mac access-list extended mac1
(CN1610) (Config-mac-access-list)#permit 00:00:00:00:aa:bb
ff:ff:ff:ff:00:00 any rate-limit 32 16
(CN1610) (Config-mac-access-list)#exit
```

mac access-group

This command either attaches a specific MAC Access Control List (ACL) identified by *name* to an interface or range of interfaces, or associates it with a VLAN ID, in a given direction. The *name* parameter must be the name of an existing MAC ACL.

An optional sequence number may be specified to indicate the order of this mac access list relative to other mac access lists already assigned to this interface and direction. A lower number indicates higher precedence order. If a sequence number is already in use for this interface and direction, the specified mac access list replaces the currently attached mac access list using that sequence number. If the sequence number is not specified for this command, a sequence number that is one greater than the highest sequence number currently in use for this interface and direction is used.

This command specified in 'Interface Config' mode only affects a single interface, whereas the 'Global Config' mode setting is applied to all interfaces. The VLAN keyword is only valid in the 'Global Config' mode.

An optional *control-plane* is specified to apply the MAC ACL on CPU port. The control packets like BPDU are also dropped because of the implicit deny all rule added to the end of the list. To overcome this, permit rules must be added to allow the control packets.

Note

The keyword *control-plane* is only available in Global Config mode.

Format	`mac access-group` *`name`* {{*`control-plane`*|`in`|`out`} `vlan` *`vlan-id`* {`in`|`out`}}
Modes	◆ Global Config ◆ Interface Config

Parameter	Description
name	The name of the Access Control List.
vlan-id	A VLAN ID associated with a specific IP ACL in a given direction.

The following shows an example of the command.

```
(CN1610)(Config)#mac access-group mac1 control-plane
```

no mac access-group

This command removes a MAC ACL identified by *`name`* from the interface in a given direction.

Format	`no mac access-group` *`name`* {{*`control-plane`*|`in`|`out`} `vlan` *`vlan-id`* {`in`|`out`}}
Modes	◆ Global Config ◆ Interface Config

The following shows an example of the command.

```
(CN1610)(Config)#no mac access-group mac1 control-plane
```

show mac access-lists

This command displays a MAC access list and all of the rules that are defined for the MAC ACL. Use the `[name]` parameter to identify a specific MAC ACL to display. The `rate-limit` attribute displays committed rate and committed burst size.

Note

The command output varies based on the match criteria configured within the rules of an ACL.

Format	`show mac access-lists` *`[name]`*
Mode	Privileged EXEC

Term	Definition
Rule Number	The ordered rule number identifier defined within the MAC ACL.
Action	The action associated with each rule. The possible values are Permit or Deny.
Source MAC Address	The source MAC address for this rule.
Source MAC Mask	The source MAC mask for this rule.
Committed Rate	The committed rate defined by the rate-limit attribute.
Committed Burst Size	The committed burst size defined by the rate-limit attribute.
Destination MAC Address	The destination MAC address for this rule.
Ethertype	The Ethertype keyword or custom value for this rule.
VLAN ID	The VLAN identifier value or range for this rule.
COS	The COS (802.1p) value for this rule.
Log	Displays when you enable logging for the rule.
Assign Queue	The queue identifier to which packets matching this rule are assigned.
Mirror Interface	The slot/port to which packets matching this rule are copied.
Redirect Interface	The slot/port to which packets matching this rule are forwarded.
Time Range Name	Displays the name of the time-range if the MAC ACL rule has referenced a time range.

Term	Definition
Rule Status	Status (Active/Inactive) of the MAC ACL rule.

The following shows example CLI display output for the command.

```
(CN1610) #show mac access-lists mac1

ACL Name: mac1

Outbound Interface(s): control-plane

Rule Number: 1
Action..................................... permit
Source MAC Address......................... 00:00:00:00:AA:BB
Source MAC Mask............................ FF:FF:FF:FF:00:00
Committed Rate............................. 32
Committed Burst Size....................... 16
```

IP Access Control List Commands

This section describes the commands you use to configure IP Access Control List (ACL) settings. IP ACLs ensure that only authorized users have access to specific resources and block any unwarranted attempts to reach network resources.

The following rules apply to IP ACLs:

- FASTPATH software does not support IP ACL configuration for IP packet fragments.
- The maximum number of ACLs you can create is hardware dependent. The limit applies to all ACLs, regardless of type.
- The maximum number of rules per IP ACL is hardware dependent.
- Wildcard masking for ACLs operates differently from a subnet mask. A wildcard mask is in essence the inverse of a subnet mask. With a subnet mask, the mask has ones (1's) in the bit positions that are used for the network address, and has zeros (0's) for the bit positions that are not used. In contrast, a wildcard mask has (0's) in a bit position that must be checked. A **1** in a bit position of the ACL mask indicates the corresponding bit can be ignored.

access-list

This command creates an IP Access Control List (ACL) that is identified by the access list number, which is 1-99 for standard ACLs or 100-199 for extended ACLs.

IP Standard ACL:

Format	`access-list` *`1-99`* `[rule` *`1-1023`*`] {deny | permit} {every |` *`srcip srcmask`*`} [log] [time-range` *`time-range-name`*`][assign-queue` *`queue-id`*`] [{mirror | redirect}` *`slot/port`*`]`
Mode	Global Config

IP Extended ACL:

Format	access-list *100-199* [rule *1-1023*] {deny | permit} {every | {{eigrp | gre | icmp | igmp | ip | ipinip | ospf | pim | tcp | udp | *0 -255*} {*srcip* srcmask|any|host *srcip*}[range {*portkey*|*startport*} {*portkey*|*endport*} {eq|neq|lt|gt} {*portkey*|*0-65535*}{*dstip dstmask*|any|host *dstip*}[{range {*portkey*|*startport*} {*portkey*|*endport*} | {eq | neq | lt | gt} {*portkey* | *0-65535*}] [flag [+fin | -fin] [+syn | -syn] [+rst | -rst] [+psh | -psh] [+ack | -ack] [+urg | -urg] [established]] [icmp-type *icmp-type* [icmp-code *icmp-code*] | icmp-message *icmp-message*] [igmp-type *igmp-type*] [fragments] [precedence *precedence* | tos *tos* [tosmask] | dscp *dscp*]}} [time-range *time-range-name*] [log] [assign-queue *queue-id*] [{mirror | redirect} slot/port] [rate-limit *rate burst-size*]
Mode	Global Config

Note

IPv4 extended ACLs have the following limitations for egress ACLs:

- Match on port ranges is not supported.
- The rate-limit command is not supported.

Parameter	Description
1-99 or *100-199*	Range 1 to 99 is the access list number for an IP standard ACL. Range 100 to 199 is the access list number for an IP extended ACL.
[rule *1-1023*]	Specifies the IP access list rule.
{deny | permit}	Specifies whether the IP ACL rule permits or denies an action.
every	Match every packet.
{eigrp | gre | icmp | igmp | ip | ipinip | ospf | pim | tcp | udp | *0 -255*}	Specifies the protocol to filter for an extended IP ACL rule.

Parameter	Description
srcip *srcmask*|any|host *scrip*	Specifies a source IP address and source netmask for match condition of the IP ACL rule. Specifying any specifies *srcip* as 0.0.0.0 and *srcmask* as 255.255.255.255. Specifying host *A.B.C.D* specifies *srcip* as A.B.C.D and *srcmask* as 0.0.0.0.

Parameter	Description
{{range{portkey|startport}{portkey|endport}|{eq|neq|lt|gt}{*portkey* | *0-65535*}*]*	**Note** This option is available only if the protocol is TCP or UDP. Specifies the source layer 4 port match condition for the IP ACL rule. You can use the port number, which ranges from 0-65535, or you specify the *portkey*, which can be one of the following keywords: ◆ For TCP: *bgp*, *domain*, *echo*, *ftp*, *ftp-data*, *http*, *smtp*, *telnet*, *www*, *pop2*, *pop3*. ◆ For UDP: *domain, echo, ntp, rip, snmp, tftp*, *time*, and *who*. For both TCP and UDP, each of these keywords translates into its equivalent port number, which is used as both the start and end of a port range. If *range* is specified, the IP ACL rule matches only if the layer 4 port number falls within the specified portrange. The *startport* and *endport* parameters identify the first and last ports that are part of the port range. They have values from 0 to 65535. The ending port must have a value equal or greater than the starting port. The starting port, ending port, and all ports in between will be part of the layer 4 port range. When *eq* is specified, the IP ACL rule matches only if the layer 4 port number is equal to the specified port number or portkey. When *lt* is specified, IP ACL rule matches if the layer 4 port number is less than the specified port number or portkey. It is equivalent to specifying the range as 0 to <specified port number – 1>. When *gt* is specified, the IP ACL rule matches if the layer 4 port number is greater than the specified port number or portkey. It is equivalent to specifying the range as <specified port number + 1> to 65535. When *neq* is specified, IP ACL rule matches only if the layer 4 port number is not equal to the

Parameter	Description
dstip *dstmask*|any|host *dstip*	Specifies a destination IP address and netmask for match condition of the IP ACL rule. Specifying any implies specifying *dstip* as 0.0.0.0 and *dstmask* as 255.255.255.255. Specifying host A.B.C.D implies *dstip* as A.B.C.D and *dstmask* as 0.0.0.0.
[precedence *precedence* | tos *tos* [*tosmask*] | dscp *dscp*]	Specifies the TOS for an IP ACL rule depending on a match of precedence or DSCP values using the parameters *dscp*, *precedence*, *tos/tosmask*. **Note** *tosmask* is an optional parameter.
flag [+fin | -fin] [+syn | -syn] [+rst | -rst] [+psh | -psh] [+ack | -ack] [+urg | -urg] [established]	**Note** This option is available only if the protocol is tcp. Specifies that the IP ACL rule matches on the TCP flags. When +<tcpflagname> is specified, a match occurs if the specified <tcpflagname> flag is set in the TCP header. When -<tcpflagname> is specified, a match occurs if the specified <tcpflagname> flag is *NOT* set in the TCP header. When established is specified, a match occurs if the specified RST or ACK bits are set in the TCP header. Two rules are installed in the hardware when the established option is specified.

Parameter	Description
[icmp-type *icmp-type* [icmp-code *icmp-code*] | icmp-message *icmp-message*]	**Note** This option is available only if the protocol is icmp. Specifies a match condition for ICMP packets. When *icmp-type* is specified, the IP ACL rule matches on the specified ICMP message type, a number from 0 to 255. When *icmp-code* is specified, the IP ACL rule matches on the specified ICMP message code, a number from 0 to 255. Specifying *icmp-message* implies that both *icmp-type* and *icmp-code* are specified. The following icmp-messages are supported: *echo*, *echo-reply*, *host-redirect*, *mobile-redirect*, *net-redirect*, *net-unreachable*, *redirect*, *packet-too-big*, *port-unreachable*, *source-quench*, *router-solicitation*, *router-advertisement*, *time-exceeded*, *ttl-exceeded* and *unreachable*.
igmp-type *igmp-type*	This option is available only if the protocol is igmp. When *igmp-type* is specified, the IP ACL rule matches on the specified IGMP message type, a number from 0 to 255.
fragments	Specifies that the IP ACL rule matches on fragmented IP packets.
[log]	Specifies that this rule is to be logged.

Parameter	Description
[time-range *time-range-name*]	Allows imposing time limitation on the ACL rule as defined by the parameter *time-range-name*. If a time range with the specified name does not exist and the ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied immediately. If a time range with specified name exists and the ACL containing this ACL rule is applied to an interface or bound to a VLAN, the ACL rule is applied when the time-range with specified name becomes active. The ACL rule is removed when the time-range with specified name becomes inactive. For information about configuring time ranges, see "Time Range Commands for Time-Based ACLs" on page 687.
[assign-queue *queue-id*]	Specifies the assign-queue, which is the queue identifier to which packets matching this rule are assigned.
[{mirror | redirect} slot/port]	Te mirror or redirect interface which is the slot/port to which packets matching this rule are copied or forwarded, respectively.
[rate-limit *rate burst-size*]	Specifies the allowed rate of traffic as per the configured rate in kbps, and burst-size in kbytes.

no access-list

This command deletes an IP ACL that is identified by the parameter *accesslistnumber* from the system. The range for *accesslistnumber* 1-99 for standard access lists and 100-199 for extended access lists.

Format	no access-list *accesslistnumber* [rule *1-1023*]
Mode	Global Config

ip access-list

This command creates an extended IP Access Control List (ACL) identified by *name*, consisting of classification fields defined for the IP header of an IPv4 frame. The *name* parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the IP access list. The rate-limit attribute configures the committed rate and the committed burst size.

If an IP ACL by this name already exists, this command enters IPv4-Access_List config mode to allow updating the existing IP ACL.

Note
The CLI mode changes to IPv4-Access-List Config mode when you successfully execute this command.

Format	`ip access-list` *name*
Mode	Global Config

no ip access-list

This command deletes the IP ACL identified by name from the system.

Format	`no ip access-list` *name*
Mode	Global Config

ip access-list rename

This command changes the name of an IP Access Control List (ACL). The *name* parameter is the names of an existing IP ACL. The new*name* parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the IP access list.

This command fails is an IP ACL by the name new*name* already exists.

Format	`ip access-list rename` *name newname*
Mode	Global Config

{deny | permit} (IP ACL)

This command creates a new rule for the current IP access list. Each rule is appended to the list of configured rules for the list. A rule may either deny or permit traffic according to the specified classification fields. At a minimum, either the every keyword or the protocol, source address, and destination address

values must be specified. The source and destination IP address fields may be specified using the keyword any to indicate a match on any value in that field. The remaining command parameters are all optional, but the most frequently used parameters appear in the same relative order as shown in the command format.

Format	{deny | permit} {every | {{eigrp | gre | icmp | igmp | ip | ipinip | ospf | pim | tcp | udp | *0 -255*} {srcip *srcmask* | any | host *srcip*} [{range {*portkey* | *startport*} {*portkey* | *endport*} | {eq | neq | lt | gt} {*portkey* | *0-65535*}] {*dstip dstmask* | any | host *dstip*} [{range {*portkey* | *startport*} {*portkey* | *endport*} | {eq | neq | lt | gt} {*portkey* | *0-65535*}] [flag [+fin | -fin] [+syn | -syn] [+rst | -rst] [+psh | -psh] [+ack | -ack] [+urg | -urg] [established]] [icmp-type *icmp-type* [icmp-code icmp-code] | icmp-message icmp-message] [igmp-type igmp-type] [fragments] [precedence *precedence* | tos *tos* [*tosmask*] | dscp *dscp*]}} [time-range *time-range-name*] [log] [assign-queue *queue-id*] [{mirror | redirect} slot/port] [rate-limit *rate burst-size*]
Mode	Ipv4-Access-List Config

Note

The **no** form of this command is not supported, since the rules within an IP ACL cannot be deleted individually. Rather, the entire IP ACL must be deleted and respecified.

Note

An implicit **deny all** IP rule always terminates the access list.

Note

For IPv4, the following are not supported for egress ACLs:

- A match on port ranges.
- The rate-limit command.

The time-range parameter allows imposing time limitation on the IP ACL rule as defined by the specified time range. If a time range with the specified name does not exist and the ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied immediately. If a time range with specified name exists and the ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied when the time-range

with specified name becomes active. The ACL rule is removed when the time-range with specified name becomes inactive. For information about configuring time ranges, see “Time Range Commands for Time-Based ACLs” on page 687.

The `assign-queue` parameter allows specification of a particular hardware queue for handling traffic that matches this rule. The allowed *`queue-id`* value is 0-(n-1), where n is the number of user configurable queues available for the hardware platform. The *`assign-queue`* parameter is valid only for a `permit` rule.

The **permit** command’s optional attribute **rate-limit** allows you to permit only the allowed rate of traffic as per the configured rate in kbps, and burst-size in kbytes.

Parameter	**Description**
{deny | permit}	Specifies whether the IP ACL rule permits or denies the matching traffic.
Every	Match every packet.
{`eigrp` | `gre` | `icmp` | `igmp` | `ip` | `ipinip` | `ospf` | `pim` | `tcp` | `udp` | *`0 -255`*}	Specifies the protocol to match for the IP ACL rule.
srcip srcmask | any | host *`srcip`*	Specifies a source IP address and source netmask to match for the IP ACL rule. Specifying “any” implies specifying *srcip* as “0.0.0.0” and *srcmask* as “255.255.255.255”. Specifying “host A.B.C.D” implies *srcip* as “A.B.C.D” and *srcmask* as “0.0.0.0”.

Parameter	Description
[{range {*portkey*|*startport*} {*portkey*|*endport*}|{eq|neq|lt|gt} {*portkey*|*0-65535*}]	**Note** This option is available only if the protocol is tcp or udp. Specifies the layer 4 port match condition for the IP ACL rule. Port number can be used, which ranges from 0-65535, or the portkey, which can be one of the following keywords: ◆ For tcp protocol: bgp, domain, echo, ftp, ftp-data, http, smtp, telnet, www, pop2, pop3 ◆ For udp protocol: domain, echo, ntp, rip, snmp, tftp, time, who Each of these keywords translates into its equivalent port number. When range is specified, the IP ACL rule matches only if the layer 4 port number falls within the specified port range. The startport and endport parameters identify the first and last ports that are part of the port range. They have values from 0 to 65535. The ending port must have a value equal to or greater than the starting port. The starting port, ending port, and all ports in between will be part of the layer 4 port range. When eq is specified, IP ACL rule matches only if the layer 4 port number is equal to the specified port number or portkey. When lt is specified, IP ACL rule matches if the layer 4 port number is less than the specified port number or portkey. It is equivalent to specifying the range as 0 to <specified port number – 1>. When gt is specified, IP ACL rule matches if the layer 4 port number is greater than the specified port number or portkey. It is equivalent to specifying the range as <specified port number + 1> to 65535. When neq is specified, IP ACL rule matches only if the layer 4 port number is not equal to the specified port number or port key. Two rules are added in the hardware one with range equal to 0 to <specified port number _- 1> and one with range equal to <<specified port number _+ 1 to 65535>>.

Parameter	Description
dstip dstmask | any | host *dstip*	Specifies a destination IP address and netmask for match condition of the IP ACL rule. Specifying any implies specifying dstip as 0.0.0.0 and dstmask as 255.255.255.255. Specifying host A.B.C.D implies dstip as A.B.C.D and dstmask as 0.0.0.0.
[precedence *precedence* | tos *tos* [*tosmask*] | dscp *dscp*]	Specifies the TOS for an IP ACL rule depending on a match of precedence or DSCP values using the parameters *dscp, precedence*, *tos/tosmask.* tosmask is an optional parameter.
flag [+fin | -fin] [+syn | -syn] [+rst | -rst] [+psh | -psh] [+ack | -ack] [+urg | -urg] [established]	Specifies that the IP ACL rule matches on the tcp flags. When +<tcpflagname> is specified, a match occurs if specified <tcpflagname> flag is set in the TCP header. When -<tcpflagname> is specified, a match occurs if specified <tcpflagname> flag is NOT set in the TCP header. When established is specified, a match occurs if either the specified RST or ACK bits are set in the TCP header. Two rules are installed in hardware to when the established option is specified. This option is available only if protocol is tcp.

Parameter	Description
[icmp-type *icmp-type* [icmp-code *icmp-code*] | icmp-message *icmp-message*]	**Note** This option is available only if the protocol is ICMP. Specifies a match condition for ICMP packets. When *icmp-type* is specified, IP ACL rule matches on the specified ICMP message type, a number from 0 to 255. When *icmp-code* is specified, IP ACL rule matches on the specified ICMP message code, a number from 0 to 255. Specifying *icmp-message* implies both *icmp-type* and *icmp-code* are specified. The following icmp-messages are supported: echo, echo-reply, host-redirect, mobile-redirect, net-redirect, net-unreachable, redirect, packet-too-big, port-unreachable, source-quench, router-solicitation, router-advertisement, time-exceeded, ttl-exceeded and unreachable. The ICMP message is decoded into corresponding ICMP type and ICMP code within that ICMP type.
igmp-type *igmp-type*	**Note** This option is visible only if the protocol is IGMP. When *igmp-type* is specified, the IP ACL rule matches on the specified IGMP message type, a number from 0 to 255.
fragments	Specifies that IP ACL rule matches on fragmented IP packets.
log	Specifies that this rule is to be logged.

Parameter	Description
time-range *time-range-name*	Allows imposing a time limitation on the ACL rule as defined by the parameter time-range-name. If a time range with the specified name does not exist and the ACL containing this ACL rule is applied to an interface or bound to a VLAN, the ACL rule is applied immediately. If a time range with specified name exists and the ACL containing this ACL rule is applied to an interface or bound to a VLAN, the ACL rule is applied when the time-range with specified name becomes active. The ACL rule is removed when the time-range with specified name becomes inactive.
assign-queue *queue-id*	Specifies the assign-queue, which is the queue identifier to which packets matching this rule are assigned.
{mirror | redirect} *unit/slot/ port*	Specifies the mirror or redirect interface which is the unit/slot/port to which packets matching this rule are copied or forwarded, respectively.
rate-limit *rate burst-size*	Specifies the allowed rate of traffic as per the configured rate in kbps, and burst-size in kbytes.

The following shows an example of the command.

```
(CN1610) (Config)#ip access-list ip1

(CN1610) (Config-ipv4-acl)#permit icmp any any rate-limit 32 16

(CN1610) (Config-ipv4-acl)#exit
```

ip access-group

This command either attaches a specific IP Access Control List (ACL) identified by *accesslistnumber* or *name* to an interface, range of interfaces, or all interfaces; or associates it with a VLAN ID in a given direction. The parameter *name* is the name of the Access Control List.

An optional sequence number may be specified to indicate the order of this IP access list relative to other IP access lists already assigned to this interface and direction. A lower number indicates higher precedence order. If a sequence

number is already in use for this interface and direction, the specified access list replaces the currently attached IP access list using that sequence number. If the sequence number is not specified for this command, a sequence number that is one greater than the highest sequence number currently in use for this interface and direction is used.

An optional *control-plane* is specified to apply the ACL on CPU port. The IPv4 control packets like RADIUS and TACACS+ are also dropped because of the implicit **deny all** rule added at the end of the list. To overcome this, permit rules must be added to allow the IPv4 control packets.

Note
The keyword *control-plane* is only available in Global Config mode.

Default	none
Format	`ip access-group {`*`accesslistnumber`*`|`*`name`*`} {{`*`control-plane`*`|`*`in`*`|`*`out`*`}|vlan `*`vlan-id`*` {in|out}}`
Modes	◆ Interface Config ◆ Global Config

Parameter	Description
accesslistnumber	Identifies a specific IP ACL. The range is 1 to 199.
vlan-id	A VLAN ID associated with a specific IP ACL in a given direction.
name	The name of the Access Control List.

The following shows an example of the command.

```
(CN1610) (Config)#ip access-group ip1 control-plane
```

no ip access-group

This command removes a specified IP ACL from an interface.

Default	none
Format	`no ip access-group {`*`accesslistnumber`*`|`*`name`*`} {{`*`control-plane`*`|`*`in`*`|`*`out`*`}|vlan `*`vlan-id`*` {in|out}}`

Mode	◆ Interface Config ◆ Global Config

The following shows an example of the command.

```
(CN1610)(Config)#no ip access-group ip1 control-plane
```

acl-trapflags

This command enables the ACL trap mode.

Default	disabled
Format	`acl-trapflags`
Mode	Global Config

no acl-trapflags

This command disables the ACL trap mode.

Format	`no acl-trapflags`
Mode	Global Config

show ip access-lists

Use this command to view summary information about all IP ACLs configured on the switch. To view more detailed information about a specific access list, specify the ACL number or name that is used to identify the IP ACL. The **rate-limit** attribute displays committed rate and committed burst size.

Format	`show ip access-lists [`*`accesslistnumber`* `|` *`name`*`]`
Mode	Privileged EXEC

Term	Definition
ACL ID/Name	Identifies the configured ACL number or name.
Rules	Identifies the number of rules configured for the ACL.

Term	Definition
Direction	Shows whether the ACL is applied to traffic coming into the interface (ingress) or leaving the interface (egress).
Interface(s)	Identifies the interface(s) to which the ACL is applied (ACL interface bindings).
VLAN(s)	Identifies the VLANs to which the ACL is applied (ACL VLAN bindings).

If you specify an IP ACL number or name, the following information displays:

Note
Only the access list fields that you configure are displayed. Thus, the command output varies based on the match criteria configured within the rules of an ACL.

Term	Definition
Rule Number	The number identifier for each rule that is defined for the IP ACL.
Action	The action associated with each rule. The possible values are Permit or Deny.
Match All	Indicates whether this access list applies to every packet. Possible values are True or False.
Protocol	The protocol to filter for this rule.
ICMP Type	**Note** This is shown only if the protocol is ICMP. The ICMP message type for this rule.
Starting Source L4 port	The starting source layer 4 port.
Ending Source L4 port	The ending source layer 4 port.

Term	Definition
Starting Destination L4 port	The starting destination layer 4 port.
Ending Destination L4 port	The ending destination layer 4 port.
ICMP Code	**Note** This is shown only if the protocol is ICMP. The ICMP message code for this rule.
Fragments	If the ACL rule matches on fragmented IP packets.
Committed Rate	The committed rate defined by the rate-limit attribute.
Committed Burst Size	The committed burst size defined by the rate-limit attribute.
Source IP Address	The source IP address for this rule.
Source IP Mask	The source IP Mask for this rule.
Source L4 Port Keyword	The source port for this rule.
Destination IP Address	The destination IP address for this rule.
Destination IP Mask	The destination IP Mask for this rule.
Destination L4 Port Keyword	The destination port for this rule.
IP DSCP	The value specified for IP DSCP.
IP Precedence	The value specified IP Precedence.
IP TOS	The value specified for IP TOS.
Log	Displays when you enable logging for the rule.
Assign Queue	The queue identifier to which packets matching this rule are assigned.

Term	Definition
Mirror Interface	The unit/slot/port to which packets matching this rule are copied.
Redirect Interface	The unit/slot/port to which packets matching this rule are forwarded.
Time Range Name	Displays the name of the time-range if the IP ACL rule has referenced a time range.
Rule Status	Status (Active/Inactive) of the IP ACL rule.

The following shows example CLI display output for the command.

```
(CN1610) #show ip access-lists ip1

ACL Name: ip1
Inbound Interface(s): 1/0/30


Rule Number: 1
Action..................................... permit
Match All.................................. FALSE
Protocol................................... 1(icmp)
Committed Rate............................. 32
Committed Burst Size....................... 16
```

show access-lists

This command displays IP ACLs, IPv6 ACLs, and MAC access control lists information for a designated interface and direction. Instead of slot/port, `lag` *`lag-intf-num`* can be used as an alternate way to specify the LAG interface. `lag` *`lag-intf-num`* can also be used to specify the LAG interface where *`lag-intf-num`* is the LAG port number.Use the **control-plane** keyword to display the ACLs applied on the CPU port.

Format	`show access-lists interface {slot/port in|out | control-plane}`
Mode	Privileged EXEC

Term	Definition
ACL Type	Type of access list (IP, IPv6, or MAC).
ACL ID	Access List name for a MAC or IPv6 access list or the numeric identifier for an IP access list.
Sequence Number	An optional sequence number may be specified to indicate the order of this access list relative to other access lists already assigned to this interface and direction. A lower number indicates higher precedence order. If a sequence number is already in use for this interface and direction, the specified access list replaces the currently attached access list using that sequence number. If the sequence number is not specified by the user, a sequence number that is one greater than the highest sequence number currently in use for this interface and direction is used. Valid range is (1 to 4294967295).
in|out	◆ in – Display Access List information for a particular interface and the in direction. ◆ out – Display Access List information for a particular interface and the out direction.

The following shows an example of the command.

```
(CN1610) #show access-lists interface control-plane

ACL Type             ACL ID                      Sequence Number
--------          ------------------------------  ---------------
IPv6             ip61                                    1
```

show access-lists vlan

This command displays Access List information for a particular VLAN ID. The *vlan-id* parameter is the VLAN ID of the VLAN with the information to view. The *{*`in | out}` options specifies the direction of the VLAN ACL information to view.

Format	`show access-lists vlan` *`vlan-id`* `in|out`
Mode	Privileged EXEC

Term	Definition
ACL Type	Type of access list (IP, IPv6, or MAC).
ACL ID	Access List name for a MAC or IPv6 access list or the numeric identifier for an IP access list.
Sequence Number	An optional sequence number may be specified to indicate the order of this access list relative to other access lists already assigned to this interface and direction. A lower number indicates higher precedence order. If a sequence number is already in use for this interface and direction, the specified access list replaces the currently attached access list using that sequence number. If the sequence number is not specified by the user, a sequence number that is one greater than the highest sequence number currently in use for this interface and direction is used. Valid range is (1 to 4294967295).

IPv6 Access Control List Commands

This section describes the commands you use to configure IPv6 Access Control List (ACL) settings. IPv6 ACLs ensure that only authorized users have access to specific resources and block any unwarranted attempts to reach network resources.

The following rules apply to IPv6 ACLs:

- The maximum number of ACLs you create is 100, regardless of type.
- The system supports only Ethernet II frame types.
- The maximum number of rules per IPv6 ACL is hardware dependent.

ipv6 access-list

This command creates an IPv6 Access Control List (ACL) identified by *name*, consisting of classification fields defined for the IP header of an IPv6 frame. The *name* parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the IPv6 access list. The rate-limit attribute configures the committed rate and the committed burst size.

If an IPv6 ACL by this name already exists, this command enters IPv6-Access-List config mode to allow updating the existing IPv6 ACL.

Note
The CLI mode changes to IPv6-Access-List Config mode when you successfully execute this command.

Format	`ipv6 access-list` *name*
Mode	Global Config

no ipv6 access-list

This command deletes the IPv6 ACL identified by *name* from the system.

Format	`no ipv6 access-list` *name*
Mode	Global Config

ipv6 access-list rename

This command changes the name of an IPv6 ACL. The *name* parameter is the name of an existing IPv6 ACL. The *newname* parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the IPv6 access list.

This command fails is an IPv6 ACL by the name *newname* already exists.

Format	`ipv6 access-list rename name newname`
Mode	Global Config

{deny | permit} (IPv6)

This command creates a new rule for the current IPv6 access list. Each rule is appended to the list of configured rules for the list. A rule may either deny or permit traffic according to the specified classification fields. At a minimum, either the *every* keyword or the protocol, source address, and destination address values must be specified. The source and destination IPv6 address fields may be specified using the keyword *any* to indicate a match on any value in that field. The remaining command parameters are all optional, but the most frequently used parameters appear in the same relative order as shown in the command format.

Format	{deny | permit} {every | {{icmpv6 | ipv6 | tcp | udp | 0-255} {*source-ipv6-prefix/prefix-length* | any | *host source-ipv6-address*} [{range {*portkey* | *startport*} {*portkey* | *endport*} | {eq | neq | lt | gt} {*portkey* | *0-65535*}] {*destination-ipv6-prefix/prefix-length* | any | *host destination-ipv6-address*} [{range {*portkey* | *startport*} {*portkey* | *endport*} | {eq | neq | lt | gt} {*portkey* | *0-65535*}] [flag [+fin | -fin] [+syn | -syn] [+rst | -rst] [+psh | -psh] [+ack | -ack] [+urg | -urg] [established]] [flow-label value] [icmp-type *icmp-type* [icmp-code *icmp-code*] | icmp-message *icmp-message*] [routing] [fragments] [dscp *dscp*]}} [log] [assign-queue *queue-id*] [{mirror | redirect} slot/port] [rate-limit *rate burst-size*]
Mode	IPv6-Access-List Config

Note

The **no** form of this command is not supported, since the rules within an IPv6 ACL cannot be deleted individually. Rather, the entire IPv6 ACL must be deleted and respecified.

Note

An implicit **deny all IPv6** rule always terminates the access list.

The `time-range` parameter allows imposing time limitation on the IPv6 ACL rule as defined by the parameter *`time-range-name`*. If a time range with the specified name does not exist and the IPv6 ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied immediately. If a time range with specified name exists and the IPv6 ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied when the time-range with specified name becomes active. The ACL rule is removed when the time-range with specified name becomes inactive. For information about configuring time ranges, see "Time Range Commands for Time-Based ACLs" on page 687.

The assign-queue parameter allows specification of a particular hardware queue for handling traffic that matches this rule. The allowed *`queue-id`* value is 0-(n-1), where *`n`* is the number of user configurable queues available for the hardware platform. The *`assign-queue`* parameter is valid only for a permit rule.

The *`mirror`* parameter allows the traffic matching this rule to be copied to the specified slot/port, while the redirect parameter allows the traffic matching this rule to be forwarded to the specified slot/port. The *`assign-queue`* and *`redirect`* parameters are only valid for a `permit` rule.

The **permit** command's optional attribute **rate-limit** allows you to permit only the allowed rate of traffic as per the configured rate in kbps, and burst-size in kbytes.

IPv6 ACLs have the following limitations:

- Port ranges are not supported for egress IPv6 ACLs.
- The rate-limit command is not supported for egress IPv6 ACLs.

Parameter	Description
{deny | permit}	Specifies whether the IPv6 ACL rule permits or denies the matching traffic.
Every	Specifies to match every packet.
{*protocolkey* | *number*}	Specifies the protocol to match for the IPv6 ACL rule. The current list is: *`icmpv6`*, *`ipv6`*, *`tcp`*, and *`udp`*.

Parameter	Description
source-ipv6-prefix/*prefix-length* | any | *host source-ipv6-address*	Specifies a source IPv6 source address and prefix length to match for the IPv6 ACL rule. Specifying any implies specifying "::/0 " Specifying *host source-ipv6-address* implies matching the specified IPv6 address. This *source-ipv6-address* argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.

Parameter	Description
[{range {*portkey* | *startport*} {*portkey* | *endport*} | {eq | neq | lt | gt} {*portkey* | *0-65535*}]	**Note** This option is available only if the protocol is TCP or UDP. Specifies the layer 4 port match condition for the IPv6 ACL rule. A port number can be used, in the range 0-65535, or the *portkey*, which can be one of the following keywords: ◆ For TCP: *bgp*, *domain*, *echo*, *ftp*, *ftp-data*, *http*, *smtp*, *telnet*, *www*, *pop2*, *pop3* ◆ For UDP: *domain*, *echo*, *ntp*, *rip*, *snmp*, *tftp*, *time*, *who*. Each of these keywords translates into its equivalent port number. When range is specified, IPv6 ACL rule matches only if the layer 4 port number falls within the specified portrange. The *startport* and *endport* parameters identify the first and last ports that are part of the port range. They have values from 0 to 65535. The ending port must have a value equal or greater than the starting port. The starting port, ending port, and all ports in between are part of the layer 4 port range. When eq is specified, IPv6 ACL rule matches only if the layer 4 port number is equal to the specified port number or portkey. When lt is specified, IPv6 ACL rule matches if the layer 4 port number is less than the specified port number or portkey. It is equivalent to specifying the range as 0 to <specified port number – 1>. When gt is specified, IPv6 ACL rule matches if the layer 4 port number is greater than the specified port number or portkey. It is equivalent to specifying the range as <specified port number + 1> to 65535. When neq is specified, IPv6 ACL rule matches only if the layer 4 port number is not equal to the specified port number or portkey. Two rules are added in the hardware one with range equal to 0 to <specified port number - 1> and one with range equal to <<specified port number + 1 to

Parameter	Description
destination-ipv6-prefix/*prefix-length* | any | *host destination-ipv6-address*	Specifies a destination IPv6 source address and prefix length to match for the IPv6 ACL rule. Specifying any implies specifying "::/0 " Specifying *host destination-ipv6-address* implies matching the specified IPv6 address. This *destination-ipv6-address* argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
[dscp *dscp*]	Specifies the dscp value to match for for the IPv6 rule.
flag [+fin | -fin] [+syn | -syn] [+rst | -rst] [+psh | -psh] [+ack | -ack] [+urg | -urg] [established]	Specifies that the IPv6 ACL rule matches on the tcp flags. When +<tcpflagname> is specified, a match occurs if specified <tcpflagname> flag is set in the TCP header. When "-<tcpflagname>" is specified, a match occurs if specified <tcpflagname> flag is *NOT* set in the TCP header. When established is specified, a match occurs if specified either RST or ACK bits are set in the TCP header. Two rules are installed in hardware to when "established" option is specified. This option is visible only if protocol is "tcp".

Parameter	Description
[icmp-type *icmp-type* [icmp-code *icmp-code*] | icmp-message *icmp-message*]	**Note** This option is available only if the protocol is icmpv6. Specifies a match condition for ICMP packets. When *icmp-type* is specified, IPv6 ACL rule matches on the specified ICMP message type, a number from 0 to 255. When *icmp-code* is specified, IPv6 ACL rule matches on the specified ICMP message code, a number from 0 to 255. Specifying *icmp-message* implies both icmp-type and icmp-code are specified. The following icmp-messages are supported: *destination-unreachable*, *echo-reply*, *echo-request*, *header*, *hop-limit*, *mld-query*, *mld-reduction*, *mld-report*, *nd-na*, *nd-ns*, *next-header*, *no-admin*, *no-route*, *packet-too-big*, *port-unreachable*, *router-solicitation*, *router-advertisement*, *router-renumbering*, *time-exceeded*, and *unreachable*. The ICMP message is decoded into the corresponding ICMP type and ICMP code within that ICMP type.
Fragments	Specifies that IPv6 ACL rule matches on fragmented IPv6 packets (Packets that have the next header field is set to 44).
Routing	Specifies that IPv6 ACL rule matches on IPv6 packets that have routing extension headers (the next header field is set to 43).
Log	Specifies that this rule is to be logged.

Parameter	Description
`time-range` *time-range-name*	Allows imposing a time limitation on the ACL rule as defined by the parameter *time-range-name*. If a time range with the specified name does not exist and the ACL containing this ACL rule is applied to an interface or bound to a VLAN, the ACL rule is applied immediately. If a time range with the specified name exists and the ACL containing this ACL rule is applied to an interface or bound to a VLAN, the ACL rule is applied when the time-range with the specified name becomes active. The ACL rule is removed when the time-range with specified name becomes inactive.
`assign-queue` *queue-id*	Specifies the assign-queue, which is the queue identifier to which packets matching this rule are assigned.
{`mirror` | `redirect`} *unit/slot/ port*	Specifies the mirror or redirect interface which is the unit/slot/port to which packets matching this rule are copied or forwarded, respectively.
`rate-limit` *rate burst-size*	Specifies the allowed rate of traffic as per the configured rate in kbps, and burst-size in kbytes.

The following shows an example of the command.

```
(CN1610) (Config)#ipv6 access-list ip61

(CN1610) (Config-ipv6-acl)#permit udp any any rate-limit 32 16

(CN1610) (Config-ipv6-acl)#exit
```

ipv6 traffic-filter

This command either attaches a specific IPv6 ACL identified by *name* to an interface or range of interfaces, or associates it with a VLAN ID in a given direction. The *name* parameter must be the name of an existing IPv6 ACL.

An optional sequence number may be specified to indicate the order of this mac access list relative to other IPv6 access lists already assigned to this interface and direction. A lower number indicates higher precedence order. If a sequence number is already in use for this interface and direction, the specifiedIPv6 access

list replaces the currently attached IPv6 access list using that sequence number. If the sequence number is not specified for this command, a sequence number that is one greater than the highest sequence number currently in use for this interface and direction is used.

This command specified in Interface Config mode only affects a single interface, whereas the Global Config mode setting is applied to all interfaces. The `vlan` keyword is only valid in the Global Config mode.

An optional *control-plane* is specified to apply the ACL on CPU port. The IPv6 control packets like IGMPv6 are also dropped because of the implicit *deny all* rule added at the end of the list. To overcome this, permit rules must be added to allow the IPv6 control packets.

Note
The keyword *control-plane* is only available in Global Config mode.

Format	`ipv6 traffic-filter` *`name`* `{{control-plane |in|out}|vlan` *`vlan-id`* `{in|out}} [sequence` *`1-4294967295`*`]`
Modes	◆ Global Config ◆ Interface Config

The following shows an example of the command.

```
(CN1610)(Config)#ipv6 traffic-filter ip61 control-plane
```

no ipv6 traffic-filter

This command removes an IPv6 ACL identified by *`name`* from the interface(s) in a given direction.

Format	*`no`* `ipv6 traffic-filter` *`<name{{control-plane | in | out} | vlan <vlan-id> {in|out}}`*
Modes	◆ Global Config ◆ Interface Config

The following shows an example of the command.

```
(CN1610) (Config)#no ipv6 traffic-filter ip61 control-plane
```

show ipv6 access-lists

This command displays an IPv6 access list and all of the rules that are defined for the IPv6 ACL. Use the *[name]* parameter to identify a specific IPv6 ACL to display. The **rate-limit** attribute displays committed rate and committed burst size.

Format	`show ipv6 access-lists [name]`
Mode	Privileged EXEC

Note

Only the access list fields that you configure are displayed. Thus, the command output varies based on the match criteria configured within the rules of an ACL.

Term	Definition
Rule Number	The ordered rule number identifier defined within the IPv6 ACL.
Action	The action associated with each rule. The possible values are Permit or Deny.
Match All	Indicates whether this access list applies to every packet. Possible values are True or False.
Protocol	The protocol to filter for this rule.
Committed Rate	The committed rate defined by the rate-limit attribute.
Committed Burst Size	The committed burst size defined by the rate-limit attribute.
Source IP Address	The source IP address for this rule.
Source L4 Port Keyword	The source port for this rule.
Destination IP Address	The destination IP address for this rule.
Destination L4 Port Keyword	The destination port for this rule.
IP DSCP	The value specified for IP DSCP.

Term	Definition
Flow Label	The value specified for IPv6 Flow Label.
Log	Displays when you enable logging for the rule.
Assign Queue	The queue identifier to which packets matching this rule are assigned.
Mirror Interface	The slot/port to which packets matching this rule are copied.
Redirect Interface	The slot/port to which packets matching this rule are forwarded.
Time Range Name	Displays the name of the time-range if the IPv6 ACL rule has referenced a time range.
Rule Status	Status (Active/Inactive) of the IPv6 ACL rule.

The following shows example CLI display output for the command.

```
(CN1610) #show ipv6 access-lists ip61

ACL Name: ip61

Outbound Interface(s): control-plane

Rule Number: 1
Action..................................... permit
Match Every................................ FALSE
Protocol................................... 17(udp)
Committed Rate............................. 32
Committed Burst Size....................... 16
```

Time Range Commands for Time-Based ACLs

Time-based ACLs allow one or more rules within an ACL to be based on time. Each ACL rule within an ACL except for the implicit *deny all* rule can be configured to be active and operational only during a specific time period. The time range commands allow you to define specific times of the day and week in order to implement time-based ACLs. The time range is identified by a name and can then be referenced by an ACL rule defined with in an ACL.

time-range

Use this command to create a time range identified by *name*, consisting of one absolute time entry and/or one or more periodic time entries. The *name* parameter is a case-sensitive, alphanumeric string from 1 to 31 characters that uniquely identifies the time range. An alpha-numeric string is defined as consisting of only alphabetic, numeric, dash, underscore, or space characters.

If a time range by this name already exists, this command enters Time-Range config mode to allow updating the time range entries.

Note
When you successfully execute this command, the CLI mode changes to Time-Range Config mode.

Format	`time-range` *`name`*
Mode	Global Config

no time-range

This command deletes a time-range identified by *name*.

Format	`no time-range` *`name`*
Mode	Global Config

absolute

Use this command to add an absolute time entry to a time range. Only one absolute time entry is allowed per time-range. The *time* parameter is based on the currently configured time zone.

The *[start time date]* parameters indicate the time and date at which the configuration that referenced the time range starts going into effect. The time is expressed in a 24-hour clock, in the form of hours:minutes. For example, 8:00 is 8:00 am and 20:00 is 8:00 pm. The date is expressed in the format day month year. If no start time and date are specified, the configuration statement is in effect immediately.

The *[end time date]* parameters indicate the time and date at which the configuration that referenced the time range is no longer in effect. The end time and date must be after the start time and date. If no end time and date are specified, the configuration statement is in effect indefinitely.

Format	`absolute [start time date] [end time date]`
Mode	Time-Range Config

no absolute

This command deletes the absolute time entry in the time range

Format	`no absolute`
Mode	Time-Range Config

periodic

Use this command to add a periodic time entry to a time range. The *time* parameter is based off of the currently configured time zone.

The first occurrence of the *days-of-the-week* argument is the starting day(s) from which the configuration that referenced the time range starts going into effect. The second occurrence is the ending day or days from which the configuration that referenced the time range is no longer in effect. If the end days-of-the-week are the same as the start, they can be omitted

This argument can be any single day or combinations of days: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday. Other possible values are:

- daily—Monday through Sunday
- weekdays—Monday through Friday
- weekend—Saturday and Sunday

If the ending days of the week are the same as the starting days of the week, they can be omitted.

The first occurrence of the `time` argument is the starting hours:minutes which the configuration that referenced the time range starts going into effect. The second occurrence is the ending hours:minutes at which the configuration that referenced the time range is no longer in effect.

The hours:minutes are expressed in a 24-hour clock. For example, 8:00 is 8:00 am and 20:00 is 8:00 pm.

Format	`periodic` *`days-of-the-week time`* `to` *`time`*
Mode	Time-Range Config

no periodic

This command deletes a periodic time entry from a time range

Format	`no periodic` *`days-of-the-week time`* `to` *`time`*
Mode	Time-Range Config

show time-range

Use this command to display a time range and all the absolute/periodic time entries that are defined for the time range. Use the *`name`* parameter to identify a specific time range to display. When *`name`* is not specified, all the time ranges defined in the system are displayed.

Format	`show time-range [`*`name`*`]`
Mode	Privileged EXEC

The information in the following table displays when no time range name is specified.

Term	Definition
Admin Mode	The administrative mode of the time range feature on the switch
Current number of all Time Ranges	The number of time ranges currently configured in the system.
Maximum number of all Time Ranges	The maximum number of time ranges that can be configured in the system.

Term	Definition
Time Range Name	Name of the time range.
Status	Status of the time range (active/inactive)
Periodic Entry count	The number of periodic entries configured for the time range.
Absolute Entry	Indicates whether an absolute entry has been configured for the time range (Exists).

Command Index

Symbols

A

B

C

D

E

F

H

I

K

L

M

N

P

Q

R

S

T

U

V

W