Fastpath NOS CLI guide

Fastpath NOS CLI guide

Table of Contents

List of Figures

List of Tables

Chapter 1. Safety Information

1.1. Conventions

Several different typographic conventions are used throughout this manual. Refer to the following examples for common usage.

Bold type face denotes menu items, buttons and application names.

Italic type face denotes references to other sections, and the names of the folders, menus, programs, and files.

`<Enter>` type face denotes keyboard keys.

Warning information appears before the text it references and should not be ignored as the content may prevent damage to the device.

CAUTIONS APPEAR BEFORE THE TEXT IT REFERENCES, SIMILAR TO NOTES AND WARNINGS. CAUTIONS, HOWEVER, APPEAR IN CAPITAL LETTERS AND CONTAIN VITAL HEALTH AND SAFETY INFORMATION.

Indicates information that is important to know for the proper completion of a procedure, choice of an option, or completing a task.

Highlights general or useful information and tips.

1.2. Acronyms

Word	Definition
A/D	Analog to Digital
ACPI	Advanced Configuration and Power Interface
ASF	Alerting Standard Forum
Asserted	Active-high (positive true) signals are asserted when in the high electrical state (near power potential). Active-low (negative true) signals are asserted when in the low electrical state (near ground potential).
BIOS	Basic Input/Output System
BIST	Built-In Self Test
BMC	At the heart of the IPMI architecture is a microcontroller called the Baseboard management controller (BMC)
Bridge	Circuitry connecting one computer bus to another, allowing an agent on one to access the other
BSP	Bootstrap processor
Byte	8-bit quantity
CLI	Command Line Interface
CMOS	In terms of this specification, this describes the PC-AT compatible region of battery-backed 128 bytes of memory, which normally resides on the baseboard
CPU	Central Processing Unit
Deasserted	A signal is deasserted when in the inactive state. Active-low signal names have "_L" appended to the end of the signal mnemonic. Active-high signal names have no "_L" suffix. To reduce confusion when referring to active-high and active-low signals, the terms one/zero, high/low, and true/false are not used when describing signal states.
DTC	Data Transfer Controller
EEPROM	Electrically Erasable Programmable Read-Only Memory
EMP	Emergency Management Port
FRU	Field Replaceable Unit
GB	1024 MB.
GPIO	General Purpose Input/Out
HSC	Hot-Swap Controller
Hz	Hertz (1 cycle/second)
I2C	Inter-Integrated Circuit bus
IANA	Internet Assigned Numbers Authority
IBF	Input buffer
ICH	I/O Controller Hub

Word	Definition
ICMB	Intelligent Chassis Management Bus
IERR	Internal Error
IP	Internet Protocol
IPMB	Intelligent Platform Management Bus
IPMI	Intelligent Platform Management Interface
ITP	In-Target Probe
KB	1024 bytes.
KCS	Keyboard Controller Style
KVM	Keyboard, Video, Mouse
LAN	Local Area Network
LCD	Liquid Crystal Display
LCT	Lower Critical Threshold
LED	Light Emitting Diode
LNCT	Lower Non-Critical Threshold
LNRT	Lower Non-Recoverable Threshold
LPC	Low Pin Count
LSI	Large Scale Integration
LUN	Logical Unit Number
MAC	Media Access Control
MB	1024 KB
MD2	Message Digest 2 - Hashing Algorithm
MD5	Message Digest 5 - Hashing Algorithm - Higher Security
Ms	Milliseconds
Mux	Multiplexer
NIC	Network Interface Card
NMI	Nonmaskable Interrupt
NM	Node Management
OBF	Output buffer
OEM	Original Equipment Manufacturer
Ohm	Unit of electrical resistance
PDB	Power Distribution Board
PEF	Platform Event Filtering
PEP	Platform Event Paging
PERR	Parity Error
POH	Power-On Hours

Word	Definition
POST	Power-On Self Test
PWM	Pulse Width Modulation
RAC	Remote Access Card
RAM	Random Access Memory
RMCP	Remote Management Control Protocol
ROM	Read Only Memory
RTC	Real-Time Clock. Component of the chipset on the baseboard.
RTOS	Real Time Operation System
SCI	Serial Communication Interface
SDC	SCSI Daughter Card
SDR	Sensor Data Record
SEEPROM	Serial Electrically Erasable Programmable Read-Only Memory
SEL	System Event Log
SERR	System Error
SMBus	A two-wire interface based on the I2C protocol. The SMBus is a low-speed bus that provides positive addressing for devices, as well as bus arbitration
SMI	Server Management Interrupt. SMI is the highest priority nonmaskable interrupt
SMM	Server Management Mode
SMS	Server Management Software
SNMP	Simple Network Management Protocol
SOL	Serial Over LAN
UART	Universal Asynchronous Receiver/Transmitter
UCT	Upper Critical Threshold
UDP	User Datagram Protocol
UNCT	Upper Non-Critical Threshold
UNRT	Upper Non-Recoverable Threshold
WDT	Watchdog Timer
Word	16-bit quantity

1.3. Safety Information

1.3.1. Important Safety Instructions

Read all caution and safety statements in this document before performing any of the instructions.

Warnings

Heed safety instructions: Before working with the server, whether using this manual or any other resource as a reference, pay close attention to the safety instructions. Adhere to the assembly instructions in this manual to ensure and maintain compliance with existing product certifications and approvals. Use only the described, regulated components specified in this manual. Use of other products / components will void the UL listing and other regulatory approvals of the product and will most likely result in non-compliance with product regulations in the region(s) in which the product is sold.

System power on/off: The power button DOES NOT turn off the system AC power. To remove power from system, you must unplug the AC power cord from the wall outlet. Make sure the AC power cord is unplugged before opening the chassis, adding, or removing any components.

Hazardous conditions, devices and cables: Hazardous electrical conditions may be present on power, telephone, and communication cables. Turn off the server and disconnect the power cord, telecommunications systems, networks, and modems attached to the server before opening it. Otherwise, personal injury or equipment damage can result.

Electrostatic discharge (ESD) and ESD protection: ESD can damage drives, boards, and other parts. We recommend that you perform all procedures in this chapter only at an ESD workstation. If one is not available, provide some ESD protection by wearing an antistatic wrist strap attached to chassis ground any unpainted metal surface on the server when handling parts.

ESD and handling boards: Always handle boards carefully. They can be extremely sensitive to electrostatic discharge (ESD). Hold boards only by their edges. After removing a board from its protective wrapper or from the server, place the board component side up on a grounded, static free surface. Use a conductive foam pad if available but not the board wrapper. Do not slide board over any surface.

Installing or removing jumpers: A jumper is a small plastic encased conductor that slips over two jumper pins. Some jumpers have a small tab on top that can be gripped with fingertips or with a pair of fine needle nosed pliers. If the jumpers do not have such a tab, take care when using needle nosed pliers to remove or install a jumper; grip the narrow sides of the jumper with the pliers, never the wide sides. Gripping the wide sides can damage the contacts inside the jumper, causing intermittent problems with the function controlled by that jumper. Take care to grip with, but not squeeze, the pliers or other tool used to remove a jumper, or the pins on the board may bend or break.

1.4. Disclaimer

The information in this document is subject to change without notice. The manufacturer makes no representations or warranties with respect to the contents hereof and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, the manufacturer reserves the right to revise this publication and to make changes from time to time in the content hereof without obligation of the manufacturer to notify any person of such revision or changes.

For the latest information and updates please refer to www.netbergtw.com

All the illustrations in this technical guide are for reference only and are subject to change without prior notice.

Chapter 2. Console and Telnet Administration Interface

This chapter discusses many of the features used to manage the Switch and explains many concepts and important points regarding these features. Configuring the Switch to implement these concepts is discussed in detail in Chapter 8, *Switching Commands*.

2.1. Local Console Management

Local console management involves the administration of the Switch via a direct connection to the RS-232 DCE console port. This is an Out-of-band connection, meaning that it is on a different circuit than normal network communications, and thus works even when the network is down.

The local console management connection involves a terminal or PC running terminal emulation software to operate the Switch's built-in console program. Using the console program, a network administrator can manage, control, and monitor many functions of the Switch. Hardware components in the Switch allow it to be an active part of a manageable network. These components include a CPU, memory for data storage, other related hardware, and SNMP agent firmware. Activities on the Switch can be monitored with these components while the Switch can be manipulated to carry out specific tasks.

2.2. Set Up your Switch Using Console Access

Out-of-band management requires connecting a terminal, such as a VT-100 or a PC running a terminal emulation program (such as **putty**) to the RS-232 DCE console port of the Switch. Switch management using the RS-232 DCE console port is called Local Console Management to differentiate it from management done via management platforms, such as DView or HP OpenView.

Make sure the terminal or PC you are using to make this connection is configured to match these settings. If you are having problems making this connection on a PC, make sure the emulation is set to VT-100 or ANSI. If you still don't see anything, try pressing <Ctrl> + r to refresh the screen.

The first-time configuration must be carried out through a console, that is, either (a) a VT100-type serial data terminal, or (b) a computer running communications software set to emulate a VT100. The console must be connected to the Diagnostics port - an RS-232 port with a 9-socket D-shell connector and DCE-type wiring. Make the connection as follows:

1. Obtain suitable cabling for the connection.You can use a null-modem RS-232 cable or an ordinary RS-232 cable and a null-modem adapter. One end of the cable (or cable/adapter combination) must have a 9-pin D-shell connector suitable for the Diagnostics port, the other end must have a connector suitable for the console's serial communications port.

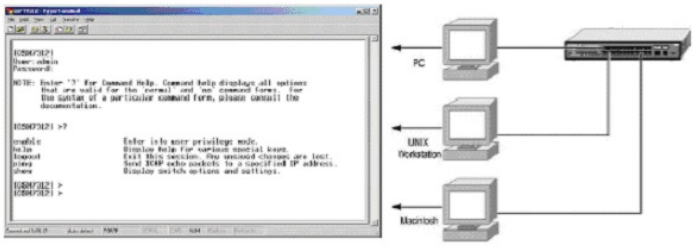
2. Power down the devices, attach the cable (or cable/adapter combination) to the correct ports and restore power.

3. Set the console to use the following communication parameters for your terminal:

   - The console port is set for the following configuration:
   - Baud rate: 9,600
   - Data width: 8 bits
   - Parity: none
   - Stop bits: 1
   - Flow Control: none

A typical console connection is illustrated below:

Figure 2.1. Console Setting Environment



2.3. Set Up your Switch Using Telnet Access

The switch has 192.168.0.1 IP address by default. Aurora 100 series Ethernet switch can be managed through any port on the device.

Once you have set an IP address for your Switch, you can use a Telnet program (in a VT-100 compatible terminal mode) to access and control the Switch. Most of the screens are identical, whether accessed through the console port or a Telnet interface.

2.4. Accessing the CLI

Once console or Telnet access is established, and the system completes the boot cycle, the User: prompt appears.

At the User: prompt, type *admin* and press ENTER. The Password: prompt appears.

1. There is no default password. Press ENTER at the password prompt if you did not change the default password.

After a successful login, the screen shows the system prompt, for example (Switch) >.

1. At the (Switch) > prompt, enter 'enable 'to enter the Privileged EXEC command mode.

2. There is no default password to enter Privileged EXEC mode. Press ENTER at the password prompt if you did not change the default password.

The command prompt changes to (Switch) #.

1. To view service network information, type *show network* and press ENTER.

Example:

```
(Switch) #show network
Interface Status.............................. Up
IP Address.................................... 192.168.0.71
Subnet Mask................................... 255.255.255.0
Default Gateway............................... 0.0.0.0
IPv6 Administrative Mode...................... Enabled
Burned In MAC Address......................... 00:05:64:30:19:10
MAC Address Type.............................. Burned In
Configured IPv4 Protocol...................... None
Configured IPv6 Protocol...................... None
IPv6 AutoConfig Mode.......................... Disabled
Management VLAN ID............................ 1
```

By default, the DHCP client on the service port is enabled. If your network has a DHCP server, then you need only to connect the switch service port to your management network to allow the switch to acquire basic network information.

Chapter 3. Introduction

FASTPATH is an off-the-shelf (Linux based) network operating system (NOS) for SMB class switches.

This document describes the CLI command of Fastpath.

This guide is universal and refers to all available commands. For exact switch capabilities, please refer to particular model technical specification.

Chapter 4. Using the Command-Line Interface

4.1. 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.
- ipaddrand 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 *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.

4.2. Command Conventions

The parameters for a command might include mandatory values, optional values, or keyword choices.

Parameters are order dependent.

Table 4.1. Parameter Conventions

Symbol	Example
Description	[] square brackets
	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
	Indicates a choice within an optional element.

4.3. 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 table below describes common parameter values and value formatting.

Table 4.2. Parameter Descriptions

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)
macaddr	The MAC address format is six hexadecimal numbers separated by colons, for example, 00:06:29:32:81:40.
areaid	Area IDs may be entered in dotted-decimal notation (for example, 0.0.0.1). An area ID of 0.0.0.0 is reserved for the backbone. Area IDs have the same form as IP addresses but are distinct from IP addresses. The IP network number of the sub-netted network may be used for the area ID.
routerid	The value of <router id> must be entered in 4-digit dotted-decimal notation (for example, 0.0.0.1). A router ID of 0.0.0.0 is invalid.
slot/port	This parameter denotes a valid slot number and a valid port number. For example, 0/1 represents unit number 1, slot number 0 and port number 1. The <slot/port> field is composed of a valid slot number and a valid port number separated by a forward slash (/).
logical slot/port	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.
Character strings	Use double quotation marks to identify character strings, for example, “System Name with Spaces”. An empty string (“”) is not valid.

4.4. Slot/Port Naming Convention

The Fastpath software references physical entities such as cards and ports by using a unit/slot/port naming convention.

The Fastpath software also uses this convention to identify certain logical entities, such as Port-Channel interfaces.

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.

Table 4.3. Type of Slots

Slot Type	Description
Physical slot numbers	Physical slot numbers begin with zero and are allocated up to the maximum number of physical slots.
Logical slot numbers	Logical slots immediately follow physical slots and identify port-channel (LAG) or router interfaces.
CPU slot numbers	The CPU slots immediately follow the logical slots.

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

Table 4.4. Type of Ports

Port Type	Description
Physical Ports	The physical ports for each slot are numbered sequentially starting from zero.
Logical Interfaces	Port-channel or Link Aggregation Group (LAG) interfaces are logical interfaces that are only used for bridging functions. VLAN routing interfaces are only used for routing functions. Loopback interfaces are logical interfaces that are always up. Tunnel interfaces are logical point-to-point links that carry encapsulated packets.
CPU ports	CPU ports are handled by the driver as one or more physical entities located on physical slots.

In the CLI, loopback interfaces do not use the slot/port format. To specify a loopback interface, you use the loopback ID.

4.5. 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 reenable a disabled feature or to enable a feature that is disabled by default. Only the configuration commands are available in the **no** form.

4.6. Executing Show Commands

All show commands can now be issued from any configuration mode (Global Config, Interface Config, VLAN Config, etc.). The show commands provide information about the system and feature-specific configuration, status, and statistics. In previous releases, show commands could be issued only in User EXEC or Privileged EXEC modes.

4.7. CLI Output Filtering

Many CLI show commands include considerable content to display to the user. This can make output confusing and cumbersome to parse through to find important information. The CLI Output Filtering feature allows the user when executing CLI show display commands, to specify optional arguments to filter the CLI output to display only desired information. The result is to simplify the display and make it easier for the user to find the information the user is interested in.

The main functions of the CLI Output Filtering feature are:

- Pagination Control - Support enabling/disabling paginated output for all **show** CLI commands. When disabled, the output is displayed in its entirety. When enabled, the output is displayed page-by-page such that content does not scroll off the terminal screen until the user presses a key to continue.

Although some Fastpath show commands already support pagination, the implementation is unique per command and not generic to all commands.

- Output Filtering
  - “Grep”-like control for modifying the displayed output to only show the user-desired content.
- Filter displayed output to only include lines containing a specified string match.
- Filter displayed output to exclude lines containing a specified string match.
- Filter displayed output to only include lines including and following a specified string match.
- Filter displayed output to only include a specified section of the content (e.g.,”interface 0/1”) with a configurable end-of-section delimiter.
- String matching should be case insensitive.
- Pagination, when enabled, also applies to filtered output.

Example: The following shows an example of the extensions made to the CLI show commands for the Output Filtering feature.

```
show running-config ?
<cr> Press enter to execute the command.
all Show all the running configuration on the switch.
| Output filter options
show running-config | ?
include {keyword} exclude {keyword}
section {begin end}
```

For commands for the feature, see Section 7.2, “CLI Output Filtering Commands”.

Chapter 5. Fastpath modules

Fastpath software consists of flexible modules that can be applied in various combinations to develop advanced Layer 2+ 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 Fastpath software.

The Fastpath software suite includes the following modules:

Chapter 8, *Switching Commands*

Chapter 9, *Routing Commands*

Chapter 10, *Quality of Service Commands*

Chapter 6, *Management Commands*

???

Not all modules are available for all platforms or software releases.

5.1. Command Modes

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

The command prompt changes in each command mode to help you identify the current mode. The table below describes the command modes and the prompts visible in that mode.

The command modes available on your switch depend on the software modules that are installed. For example, a switch that does not support BGPv4 does not have the BGPv4 RouterCommand Mode.

Table 5.1. CLI Command Modes

Command Mode	Prompt	Mode Description
User EXEC	Switch>	Contains a limited set of commands to view basic system information.
Privileged EXEC	Switch#	Allows you to issue any EXEC command, enter the VLAN mode, or enter the Global Configuration mode.
Global Config	Switch (Config)#	Groups general setup commands and permits you to make modifications to the running configuration.
VLAN Config	Switch (Vlan)#	Groups all the VLAN commands.
Interface Config	Switch (Interface slot/port)# Switch (Interface vlan vlan-id)# Switch (Interface lag vlan-id)# Switch (Interface Loopback id)# Switch (Interface tunnel id)# Switch (Interfaceslot/port (startrange)-slot/port(endrange)#	Manages the operation of an interface and provides access to the router interface configuration commands. 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 for the range of interfaces from ports 0/2 to 0/4, the prompt displays as follows: (Switch) (Interface 0/2-0/4)#
Line Console	Switch (config-line)#	Contains commands to configure outbound telnet settings and console interface settings, as well as to configure console login/enable authentication
Line SSH	Switch (config-ssh)#	Contains commands to configure SSH login/ enable authentication.
Line Telnet	Switch (config-telnet)#	Contains commands to configure telnet login/ enable authentication.

Command Mode	Prompt	Mode Description
AAA IAS User Config	Switch (Config-IAS-User)#	Allows password configuration for a user in the IAS database.
Mail Server Config	Switch (Mail-Server)#	Allows configuration of the e-mail server.
Policy Map Config	Switch (Config-policy-map)#	Contains the QoS Policy-Map configuration commands.
Policy Class Config	Switch (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	Switch (Config-class-map)#	Contains the QoS class map configuration commands for IPv4.
MAC Access-list Config	Switch (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	Switch (Tacacs)#	Contains commands to configure properties for the TACACS servers

The next table explains how to enter each mode. To exit a mode and return to the previous mode, enter exit. To exit to Privileged EXEC mode, press Ctrl+z.

Pressing Ctrl+z from Privileged EXEC mode exits to User EXEC mode. To exit User EXEC mode, enter logout.

Table 5.2. CLI Mode Access and Exit

Command Mode	Access Method
User EXEC	This is the first level of access.
Privileged EXEC	From the User EXEC mode, enter the *enable* command.
Global Config	From the Privileged EXEC mode, enter the *configure* command.
VLAN Config	From the Privileged EXEC mode, enter *vlan database* command.
Interface Config	From the Global Config mode, enter one of the following: interface slot/port interface vlan vlan-id interface lag lag-number interface loopback id interface tunnel id interface slot/port(startrange)-slot/port(endrange)

Command Mode	Access Method
Line Console	From the Global Config mode, enter *line console*.
Line SSH	From the Global Config mode, enter *line ssh*.
Line Telnet	From the Global Config mode, enter *line telnet*.
AAA IAS User Config	From the Global Config mode, enter *aaa ias-user username name*.
Mail Server Config	From the Global Config mode, enter *mail-server address*
Policy-Map Config	From the Global Config mode, enter *policy-map <policy-name><direction>*.
Policy-Class-Map Config	From the Policy Map mode enter *class <classname>*. Note: Classname should be created using the *class-map* command.
Class-Map Config	From the Global Config mode, enter *class-map match-all <class-map-name>*, and specify the optional keyword ipv4 or ipv6 to specify the Layer 3 protocol for this class. See Section 10.3.1, “class-map” for more information.
MAC Access-list Config	From the Global Config mode, enter *mac access-list extended name*.
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.

5.2. Command Completion and Abbreviation

Command completion finishes spelling the command when you type enough letters of a command to identify uniquely 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 there are enough letters to identify uniquely the command. You must enter all of the required keywords and parameters before you enter the command.

5.3. CLI Error Messages

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

Table 5.3. 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 is 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 identify uniquely the command.

5.4. CLI Line-Editing Conventions

The table below 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.

Table 5.4. CLI Editing Conventions

Key Sequence	Description
DEL or Backspace	Delete previous character.
Ctrl-A	Go to the beginning of the line.
Ctrl-E	Go to end of the 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 the line.
Ctrl-K	Delete to end of the line.
Ctrl-W	Delete previous word.
Ctrl-T	Transpose previous character.
Ctrl-P	Go to the previous line in the history buffer.
Ctrl-R	Rewrites or pastes the line.
Ctrl-N	Go to next line in the 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.
?	List available commands, keywords, or parameters.

5.5. Using CLI Help

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

```
(Switch)>?
enable          Enter into user privilege mode.
help            Display help for various special keys.
logout          Exit this session. Any unsaved changes are lost.
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.

```
(Switch) #network ?
mgmt_vlan              Configure the Management VLAN ID of the switch.
parms                  Configure Network Parameters of the router.
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.

```
(Switch) #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:

```
(Switch) #show m?
mac-addr-table  mac-address-table monitor
```

5.6. 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 or DHCP server on your network. For more information, see Section 6.1, “Network Interface Commands”.

Chapter 6. Management Commands

This section describes the following management commands available in the FASTPATH CLI:

6.1. Network Interface Commands

This section describes the commands you use to configure a logical interface for management access.

6.1.1. 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.

Syntax	enable
Command Mode	User EXEC

6.1.2. do (Privileged EXEC commands)

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

Syntax	do *Priv Exec Mode Command*
Mode	Global Config / Interface Config / VLAN Config / Routing Config

Example: The following is an example of the do command that executes the Privileged Exec command script list in Global Config Mode.

```
(Routing) #configure
(Routing)(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.
Routing(config)#
```

6.1.3. 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. You can specify the *none* option to clear the IPv4 address and mask and the default gateway (i.e., to reset each of these values to the default value on the switch).

Syntax	network parms {ipaddr netmask [gateway]| none}
Command Mode	Privileged EXEC

6.1.4. 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	dhcp
Syntax	network protocol {none | bootp | dhcp}
Command Mode	Privileged EXEC

6.1.5. network protocol dhcp

This command enables the DHCPv4 client on a Network port and sends DHCP client messages with the client identifier option (DHCP Option 61).

Syntax	network protocol dhcp [client-id]
Command Mode	Global Config

There is no support for the **no** form of the command **network protocol dhcp client-id**. To remove the *client-id* option from the DHCP client messages, issue the command **network protocol dhcp** without the *client-id* option. The command *network protocol none* can be used to disable the DHCP client and client-id option on the interface.

Example: The following shows an example of the command.

```
(Routing) # network protocol dhcp client-id
```

6.1.6. 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*.

Syntax	show network
Command Mode	Privileged EXEC / User EXEC

Term	Definition
Interface Status	The network interface status; it is always considered to be
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.

Term	Definition
IPv6 Administrative Mode	Whether enabled or disabled.
IPv6 Address/Length	The IPv6 address and length.
IPv6 Default Router	The IPv6 default router address.
Burned In MAC Address	The burned in MAC address used for in-band connectivity.
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.
DHCPv6 Client DUID	The DHCPv6 client configured IPv6 protocol is dhcp.
IPv6 Autoconfig Mode	Whether IPv6 Stateless address autoconfiguration is enabled or disabled.
DHCP Client Identifier	The client identifier is displayed in the output of the command only if DHCP is enabled with the client-id option on the network port.
Management VLAN ID	The VLAN ID for the management VLAN. Some network administrators use a management VLAN to isolate system management traffic from end-user data traffic.

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

```
(admin) #show network
Interface Status.............................. Always Up
IP Address.................................... 10.250.3.1
Subnet Mask................................... 255.255.255.0
Default Gateway............................... 10.250.3.3
IPv6 Administrative Mode...................... Enabled
IPv6 Prefix is ............................... fe80::210:18ff:fe82:64c/64
IPv6 Prefix is ............................... 2003::1/128
IPv6 Default Router is ....................... fe80::204:76ff:fe73:423a
Burned In MAC Address......................... 00:10:18:82:06:4C
Locally Administered MAC address.............. 00:00:00:00:00:00
MAC Address Type.............................. Burned In
Configured IPv4 Protocol ..................... None
Configured IPv6 Protocol ..................... DHCP
DHCPv6 Client DUID ........................... 00:03:00:06:00:10:18:82
:06:4C
IPv6 Autoconfig Mode.......................... Disabled
Management VLAN ID............................ 1
DHCP Client Identifier........................ 0Fastpath-0010.1882.160B-vl1
```

6.2. 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 of 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).

6.2.1. network ipv6 enable

Use this command to enable IPv6 operation on the network port.

Default	enabled
Syntax	network ipv6 enable
Command Mode	Privileged EXEC

6.2.1.1. no network ipv6 enable

Use this command to disable IPv6 operation on the network port.

Syntax	no network ipv6 enable
Command Mode	Privileged EXEC

6.2.2. network ipv6 neighbor

Use this command to add manually 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 the hardware when the corresponding interface is operationally active.

Syntax	network ipv6 neighbor ipv6-address macaddr
Command Mode	Privileged EXEC
<ipv6-address>	The IPv6 address of the neighbor or interface.

<macaddr>	The link-layer address.

6.2.2.1. no network ipv6 neighbor

Use this command to remove IPv6 neighbors from the neighbor table.

Syntax	no network ipv6 neighbor ipv6-address macaddr
Command Mode	Privileged EXEC

6.2.3. network ipv6 address

Use the options of this command to configure manually 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.

Syntax	network ipv6 address {address/prefix-length [eui64] | autoconfig | dhcp}
Command Mode	Privileged EXEC
<address>	IPv6 prefix in IPv6 global address format.
<prefix-length>	IPv6 prefix length value.
<eui64>	Formulate IPv6 address in eui64 format.
<autoconfig>	Configure stateless global address autoconfiguration capability.
<dhcp>	Configure dhcpv6 client protocol.

6.2.3.1. 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 to disable the DHCPv6 client protocol on the network port.

Syntax	no network ipv6 address {address/prefix-length [eui64] | autoconfig | dhcp}
Command Mode	Privileged EXEC

6.2.4. network ipv6 gateway

Use this command to configure IPv6 gateway (i.e. default routers) information for the network port.

Syntax	network ipv6 gateway gateway-address
Command Mode	Privileged EXEC

<gateway-address>	Gateway address in IPv6 global or link-local address format.

6.2.4.1. no network ipv6 gateway

Use this command to remove IPv6 gateways on the network port interface.

Syntax	no network ipv6 gateway
Command Mode	Privileged EXEC

6.2.5. 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
Syntax	show network ipv6 neighbors
Command 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 entry was added to the cache.
Last Updated	The time in seconds that has elapsed since 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.

Example: The following is an example of the command.

```
(Routing) #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
```

6.2.6. show network ipv6 dhcp statistics

This command displays the statistics of the DHCPv6 client running on the network management interface.

Syntax show network ipv6 dhcp statistics

Command Mode Privileged EXEC / User EXEC

Field	Description
DHCPv6 Advertisement Packets Received	The number of DHCPv6 Advertisement packets received on the network interface.
DHCPv6 Reply Packets Received	The number of DHCPv6 Reply packets received on the network interface.
Received DHCPv6 Advertisement PacketsDiscarded	The number of DHCPv6 Advertisement packets discarded on the network interface.
Received DHCPv6 Reply Packets Discarded	The number of DHCPv6 Reply packets discarded on the network interface.
DHCPv6 Malformed Packets Received	The number of DHCPv6 packets that are received malformed on the network interface.
Total DHCPv6 Packets Received	The total number of DHCPv6 packets received on the network interface.
DHCPv6 Solicit Packets Transmitted	The number of DHCPv6 Solicit packets transmitted on the network interface.
DHCPv6 Request Packets Transmitted	The number of DHCPv6 Request packets transmitted on the network interface.
DHCPv6 Renew PacketsTransmitted	The number of DHCPv6 Renew packets transmitted on the network interface.
DHCPv6 Rebind Packets Transmitted	The number of DHCPv6 Rebind packets transmitted on the network interface.
DHCPv6 Release Packets Transmitted	The number of DHCPv6 Release packets transmitted on the network interface.
Total DHCPv6 Packets Transmitted	The total number of DHCPv6 packets transmitted on the network interface.

Example: The following shows example CLI display output for the command.

```
(admin)#show network ipv6 dhcp statistics
DHCPv6 Client Statistics ------------------------
DHCPv6 Advertisement Packets Received..... 0
DHCPv6 Reply Packets Received..... 0
Received DHCPv6 Advertisement Packets Discarded..... 0
Received DHCPv6 Reply Packets Discarded..... 0
DHCPv6 Malformed Packets Received..... 0
Total DHCPv6 Packets Received..... 0
DHCPv6 Solicit Packets Transmitted..... 0
DHCPv6 Request Packets Transmitted..... 0
DHCPv6 Renew Packets Transmitted..... 0
DHCPv6 Rebind Packets Transmitted..... 0
DHCPv6 Release Packets Transmitted..... 0
Total DHCPv6 Packets Transmitted..... 0
```

6.2.7. clear network ipv6 dhcp statistics

Use this command to clear the DHCPv6 statistics on the network management interface.

Syntax	clear network ipv6 dhcp statistics
Command Mode	Privileged EXEC

6.2.8. ping ipv6

Use this command to determine whether another computer is on the network. Ping provides a synchronous response when initiated from the CLI interface.To use the command, configure the switch for network (in-band) connection. The source and target devices must have the ping utility enabled and ran 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. Use the optional size keyword to specify the size of the ping packet.

You can utilize the ping or traceroute utilities 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.
Syntax	ping ipv6 {ipv6-global-address|hostname | {interface {slot/port | vlan vlan-id | serviceport | loopback | tunnel | network} link-local-address} [size datagram-size]}
Command Mode	Privileged EXEC / User Exec

6.2.9. 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 ran 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 interface keyword to ping an interface by using the link-local address or the global IPv6 address of the interface. You can use a loopback, network port, serviceport, tunnel, or physical interface as the source. Use the optional size keyword to specify the size of the ping packet. The ipv6-address is the link-local IPv6 address of the device you want to query.

Syntax	ping ipv6 interface {slot/port | loopback loopback-id |network |serviceport |tunnel tunnel-id} {link-local-address link-local-address | ipv6-address} [size datagram-size]

Command Mode Privileged EXEC / User Exec

6.2.10. traceroute

Use the traceroute command to discover the routes that packets 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 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 of 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 the 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. Alternatively, one might send a traceroute with an address on a loopback interface as a source to test reachability back to the loopback interface address.

In the CLI, the user may specify the source either as an IPv4 address 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.

Fastpath will not accept an incoming packet, such as a traceroute response, that arrives on a routing interface if the packet is an address on a management port. Similarly, Fastpath will not accept a packet that arrives on a management interface if the packet 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

Syntax

Command 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

Parameter	Description
	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.
initTtl	Use initTtl to specify the initial time-to-live (TTL), the maximum number of router hops between the local and remote system. The range is 1 to 255.
maxTtl	Use maxTtle to specify the maximum TTL. The range is 1 to 255.
maxFail	Use maxFail to terminate the traceroute after failing to receive a response for this number of consecutive probes. The range is 1 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. The range is 1 to 60 seconds.
count	Use the optional count parameter to specify the number of probes to send for each TTL value. The 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. The 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. The range is 11 to 39906 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.

Example: traceroute Success:

```
(Routing) # 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
```

Example: traceroute ipv6 Success

```
(Routing) # 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
Hop Count = 1 Last TTL = 5 Test attempt = 6 Test Success = 6
```

The above command can also be executed with the optional ipv6 parameter as follows: (Routing) # traceroute ipv6 2001::2 initTtl 1 maxTtl 4 maxFail 0 interval 1 count 3 port 33434 size 43

Example: traceroute Failure:

```
(Routing) # 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
```

Example: traceroute ipv6 Failure

```
(Routing) # 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
```

6.2.11. traceroute ipv6

Use this command to discover the routes that packets take when traveling to their destination through the network on a hop-by-hop basis. The ipv6-address parameter must be a valid IPv6 address. The optional port parameter is the UDP port used as the destination of packets sent as part of the traceroute. This port should be an unused port on the destination system. The range for port is 0 (zero) to 65535.The default value is 33434.

Syntax	traceroute ipv6 ipv6-address | hostname [port]}
Command Mode	Privileged EXEC

6.3. 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.

6.3.1. configuration

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.

Syntax	configuration
Command Mode	Privileged EXEC

6.3.2. 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.

Syntax	line {console | telnet | ssh}
Command Mode	Global Config
<console>	Console terminal line.
<telnet>	Virtual terminal for remote console access (Telnet).
<ssh>	Virtual terminal for secured remote console access (SSH).

Example: The following shows an example of the CLI command.

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

6.3.3. serial baudrate

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

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

6.3.3.1. no serial baudrate

This command sets the communication rate of the terminal interface.

Syntax	no serial baudrate

Command Mode	Line Config

6.3.4. 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
Syntax	serial timeout 0-160
Command Mode	Line Config

6.3.4.1. no serial timeout

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

Syntax	no serial timeout
Command Mode	Line Config

6.3.5. show serial

This command displays serial communication settings for the switch.

Syntax	show serial
Command Mode	Privileged EXEC / User EXEC

Parameter	Description
Serial Port Login Timeout (minutes)	The time, in minutes, of inactivity on a Serial port connection, after which the Switch will close the connection. Any numeric value between 0 and 160 is allowed; the factory default is 5. A value of 0 disables the timeout.
Baud Rate (bps)	The default baud rate at which the serial port will try to connect. The available values are 2400, 4800, 9600, 19200, 38400,57600, and 115200 baud. The factory default is 115200 baud.
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 Type	The Parity Method used on the Serial Port. The Parity Method is always None.

6.4. 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.

6.4.1. 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
Syntax	ip telnet server enable
Command Mode	Privileged EXEC

6.4.1.1. 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.

Syntax	no ip telnet server enable
Command Mode	Privileged EXEC

6.4.2. 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 line mode where, by default, the operational mode is character mode. The localecho option enables local echo.

Syntax	telnet ip-address|hostname port [debug] [line] [localecho]
Command Mode	Privileged EXEC / User EXEC

6.4.3. 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.

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

Syntax	transport input telnet
Command Mode	Line Config

6.4.3.1. no transport input telnet

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

Syntax	no transport input telnet
Command Mode	Line Config

6.4.4. 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
Syntax	transport output telnet
Command Mode	Line Config

6.4.4.1. no transport output telnet

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

Syntax	no transport output telnet
Command Mode	Line Config

6.4.5. 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
Syntax	session-limit 0-5
Command Mode	Line Config

6.4.5.1. no session-limit

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

Syntax	no session-limit

Command Mode	Line Config

6.4.6. session-timeout

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

Default	5
Syntax	session-timeout 1-160
Command Mode	Line Config

6.4.6.1. no session-timeout

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

Syntax	no session-timeout
Command Mode	Line Config

6.4.7. 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
Syntax	telnetcon maxsessions 0-5
Command Mode	Privileged EXEC

6.4.7.1. no telnetcon maxsessions

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

Syntax	no telnetcon maxsessions
Command Mode	Privileged EXEC

6.4.8. 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.

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
Syntax	telnetcon timeout 1-160
Command Mode	Privileged EXEC

6.4.8.1. no telnetcon timeout

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

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.

Syntax	no telnetcon timeout
Command Mode	Privileged EXEC

6.4.9. 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.

Syntax	show telnet
Command Mode	Privileged EXEC / User EXEC

Parameter	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.

6.4.10. 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.

Syntax	show telnetcon
Command Mode	Privileged EXEC / User EXEC

Parameter	Definition
Remote Connection Login Timeout (minutes)	This object indicates the number of minutes a remote connection session is allowed to remain inactive before

Parameter	Definition
	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.
Allow New Telnet Sessions	New Telnet sessions will not be allowed when this field is set to no. The factory default value is yes.

6.5. 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.

The system allows a maximum of 5 SSH sessions.

6.5.1. 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
Syntax	ip ssh
Command Mode	Privileged EXEC

6.5.2. 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	1 and 2
Syntax	ip ssh protocol [1] [2]
Command Mode	Privileged EXEC

6.5.3. 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	disabled
Syntax	ip ssh server enable
Command Mode	Privileged EXEC

6.5.3.1. no ip ssh server enable

This command disables the IP secure shell server.

Syntax	no ip ssh server enable
Command Mode	Privileged EXEC

6.5.4. 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
Syntax	sshcon maxsessions 0-5
Command Mode	Privileged EXEC

6.5.4.1. no sshcon maxsessions

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

Syntax	no sshcon maxsessions
Command Mode	Privileged EXEC

6.5.5. 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 reaccessed. Also, any keystroke activates the new timeout duration.

Default	5
Syntax	sshcon timeout 1-160
Command Mode	Privileged EXEC

6.5.5.1. 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.

Syntax	no sshcon timeout
Command Mode	Privileged EXEC

6.5.6. show ip ssh

This command displays the ssh settings.

Syntax	show ip ssh

Command Mode Privileged EXEC

Parameter	Definition
Administrative Mode	This field indicates whether the administrative mode of SSH is enabled or disabled.
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.

6.6. 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.

6.6.1. 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.

Syntax	crypto key generate rsa
Command Mode	Global Config

6.6.1.1. no crypto key generate rsa

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

Syntax	no crypto key generate rsa
Command Mode	Global Config

6.6.2. 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.

Syntax	crypto key generate dsa
Command Mode	Global Config

6.6.2.1. no crypto key generate dsa

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

Syntax	no crypto key generate dsa
Command Mode	Global Config

6.7. HyperText Transfer Protocol Commands

This section describes the commands you use to configure HyperText Transfer Protocol (HTTP) and secure HTTP access to the switch. Access to the switch by using a Web browser is enabled by default. Everything you can view and configure by using the CLI is also available by using the Web.

6.7.1. ip http accouting exec, ip https accouting exec

This command applies user exec (start-stop/stop-only) accounting list to the line methods HTTP and HTTPS.

The user exec accounting list should be created using the command „aaa accounting“..

Syntax	ip {http|https} accounting exec {default|listname}
Command Mode	Global Config
<http/https>	The line method for which the list needs to be applied.
<default>	The default list of methods for authorization services.
<listname>	An alphanumeric character string used to name the list of accounting methods.

6.7.1.1. no ip http/https accounting exec

This command deletes the authorization method list.

Syntax	no ip {http|https} accounting exec {default|listname}
Command Mode	Global Config

6.7.2. ip http authentication

Use this command to specify authentication methods for http server users. The default configuration is the local user database is checked. This action has the same effect as the command **ip http authentication local**.

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. For example, if none is specified as an authentication method after *radius*, no authentication is used if the RADIUS server is down.

Default	local
Syntax	ip http authentication method1 [method2 …]
Command Mode	Global Config

<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.

Example: The following example configures the http authentication

```
(switch)(config) # ip http authentication radius local
```

6.7.2.1. no ip http authentication

Use this command to return to the default.

Syntax	no ip http authentication
Command Mode	Global Config

6.7.3. ip https authentication

Use this command to specify authentication methods for https server users. The default configuration is the local user database is checked. This action has the same effect as the command *ip https authentication local*. 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. For example, if *none* is specified as an authentication method after radius, no authentication is used if the RADIUS server is down.

Default	local
Syntax	ip https authentication method1 [method2 …]
Command Mode	Global Config
<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.

Example: The following example configures the https authentication

```
(switch)(config) # ip https authentication radius local
```

6.7.3.1. no ip https authentication

Use this command to return to the default.

Syntax	no ip https authentication
Command Mode	Global Config

6.7.4. ip http server

This command enables access to the switch through the Web interface. When access is enabled, the user can login to the switch from the Web interface. When access is disabled, the user cannot login to the swtich's Web server. Disabling the Web interface takes effect immediately. All interfaces are affected

Default	enabled
Syntax	ip https server
Command Mode	Privileged EXEC

6.7.4.1. no ip http server

This command disables access to the switch through the Web interface. When access is disabled, the user cannot login to the switch's Web server.

Syntax	no ip http server
Command Mode	Privileged EXEC

6.7.5. ip http secure-server

This command is used to enable the secure socket layer for secure HTTP.

Default	disable
Syntax	ip http secure-server
Command Mode	Privileged EXEC

6.7.5.1. no ip http secure-server

This command is used to disable the secure socket layer for secure HTTP.

Syntax	no ip http secure-server
Command Mode	Privileged EXEC

6.7.6. ip http java

This command enables the Web Java mode. The Java mode applies to both secure and un-secure Web connections.

Default	enabled
Syntax	ip http java
Command Mode	Privileged EXEC

6.7.6.1. no ip http java

This command disables the Web Java mode. The Java mode applies to both secure and un-secure Web connections.

Syntax	ip http java
Command Mode	Privileged EXEC

6.7.7. ip http session hard-timeout

This command configures the hard timeout for un-secure HTTP sessions in hours. Configuring this value to zero will give an infinite hard-timeout. When this timeout expires, the user will be forced to re-authenticate. This timer begins on initiation of the web session and is unaffected by the activity level of the connection.

Default	24
Syntax	ip http session hard-timeout 1-168
Command Mode	Privileged EXEC

6.7.7.1. no ip http session hard-timeout

This command restores the hard timeout for un-secure HTTP sessions to the default value.

Syntax	no ip http session hard-timeout
Command Mode	Privileged EXEC

6.7.8. ip http session maxsessions

This command limits the number of allowable un-secure HTTP sessions. Zero is the configurable minimum.

Default	3
Syntax	ip http session maxsessions 0-3
Command Mode	Privileged EXEC

6.7.8.1. no ip http session maxsessions

This command restores the number of allowable un-secure HTTP sessions to the default value.

Syntax	no ip http session maxsessions
Command Mode	Privileged EXEC

6.7.9. ip http session soft-timeout

This command configures the soft timeout for un-secure HTTP sessions in minutes. Configuring this value to zero will give an infinite soft-timeout. When this timeout expires the user will be forced to re-authenticate. This timer begins on initiation of the Web session and is re-started with each access to the switch.

Default	5
Syntax	ip http session soft-timeout 1-60
Command Mode	Privileged EXEC

6.7.9.1. no ip http session soft-timeout

This command resets the soft timeout for un-secure HTTP sessions to the default value.

Syntax	no ip http session soft-timeout
Command Mode	Privileged EXEC

6.7.10. ip http secure-session hard-timeout

This command configures the hard timeout for secure HTTP sessions in hours. When this timeout expires, the user is forced to re-authenticate. This timer begins on initiation of the Web session and is unaffected by the activity level of the connection. The secure-session hard-timeout can not be set to zero (infinite).

Default	24
Syntax	ip http secure-session hard-timeout 1-168
Command Mode	Privileged EXEC

6.7.10.1. no ip http secure-session hard-timeout

This command resets the hard timeout for secure HTTP sessions to the default value.

Syntax	no ip http secure-session hard-timeout
Command Mode	Privileged EXEC

6.7.11. ip http secure-session maxsessions

This command limits the number of secure HTTP sessions. Zero is the configurable minimum.

Default	4
Syntax	ip https secure-session maxsessions 0-4

Command Mode	Privileged EXEC

6.7.11.1. no ip http secure-session maxsessions

This command restores the number of allowable secure HTTP sessions to the default value.

Syntax	no ip http secure-session maxsessions
Command Mode	Privileged EXEC

6.7.12. ip http secure-session soft-timeout

This command configures the soft timeout for secure HTTP sessions in minutes. Configuring this value to zero will give an infinite soft-timeout. When this timeout expires, you are forced to re-authenticate. This timer begins on initiation of the Web session and is re-started with each access to the switch. The secure-session soft-timeout can not be set to zero (infinite).

Default	5
Syntax	ip http secure-session soft-timeout
Command Mode	Privileged EXEC

6.7.12.1. no ip http secure-session soft-timeout

This command restores the soft timeout for secure HTTP sessions to the default value.

Syntax	no ip http secure-session soft-timeout

Command Mode::Privileged EXEC

6.7.13. ip http secure-port

This command is used to set the SSL port where port can be 1025-65535 and the default is port 443.

Default	443
Syntax	ip http secure-port portid
Command Mode	Privileged EXEC

6.7.13.1. no ip http secure-port

This command is used to reset the SSL port to the default value.

Syntax	ip https authentication method1 [method2 …]
Command Mode	Privileged EXEC

6.7.14. ip http secure-protocol

This command is used to set protocol levels (versions). The protocol level can be set to TLS1, SSL3 or to both TLS1 and SSL3.

Default	SSL3 and TLS1
Syntax	ip http secure-protocol [SSL3] [TLS1]
Command Mode	Privileged EXEC

6.7.15. show ip http

This command displays the http settings for the switch.

Syntax	show ip http
Command Mode	Privileged EXEC

Term	Description
HTTP Mode (Unsecure)	The unsecure HTTP server administrative mode.
Java Mode	The java applet administrative mode which applies to both secure and un-secure web connections.
Maximum Allowable HTTP Sessions	The number of allowable un-secure http sessions.
HTTP Session Hard Timeout	The hard timeout for un-secure http sessions in hours.
HTTP Seesion Soft Timeout	The soft timeout for un-secure http sessions in minutes.
HTTP Mode (Secure)	The secure HTTP server administrative mode.
Secure Port	The secure HTTP server port number.
Secure Protocol Level(s)	The protocol level may have the values of SSL3, TLS1, or both.
Maximum Allowable HTTPS Sessions	The number of allowable secure http sessions.
HTTPS Session Hard Timeout	The hard timeout for secure http sessions in hours.
HTTPS Session Soft Timeout	The soft timeout for secure http session in minutes.
Certificate Present	Indicates whether the secure-server certificat files are present on the device.
Certificate Generation in Progress	Indicates whether certificate generation is currently in progress.

6.8. Access Commands

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

6.8.1. 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.

Syntax	disconnect {session_id | all}
Command Mode	Privileged EXEC

6.8.2. linuxsh

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

Default	ip-port:2324
Syntax	linuxsh [ip-port]
Command Mode	Privileged Exec
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.

6.9. 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.

Syntax	show loginsession
Command Mode	Privileged EXEC

Parameter	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.

6.9.1. show loginsession long

This command displays the complete usernames of the users currently logged into the switch.

Syntax	show loginsession long
Command Mode	Privileged EXEC

Example: The following shows an example of the command.

```
(Routing) #show loginsession long
User Name
------------
admin
testuser
```

6.10. AAA 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.

You cannot delete the admin user. There is only one user allowed with read/write privileges. You can configure up to five read-only users on the system.

6.10.1. 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.
Syntax	aaa authentication login {default | list-name} method1 [method2…]
Command 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.
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 of 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. Users the list of all TRACACS servers for authentication.

Example: The following shows an example of the command.

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

6.10.1.1. no aaa authentication login

This command returns to the default.

Syntax	aaa authentication login {default | list-name}
Command Mode	Global Config

6.10.2. aaa authentication enable

Use this command to set authentication for accessing higher privilege levels. The default enable list is *enableList*. It is used by the 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 Fastpath, 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)

Example: See the examples below.

a. aaa authentication enable default enable none

b. aaa authentication enable default line none

c. aaa authentication enable default enable radius none

d. aaa authentication enable default line tacacs none

Examples **a** and **b** do not prompt for a password, however because examples **c** and **d** 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 Fastpath does not prompt for a username. In such cases, Fastpath only prompts for a password.

Fastpath 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.

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
Syntax	aaa authentication enable {default | list-name} method1 [method2…]
Command Mode	Global Config

Parameter	Definition
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…]	At least one of the following: • enable. Uses the enable password for authentication. • line. Uses the line password for authentication. • deny. Used to deny access • none. Uses no authentication. • radius. Uses the list of all RADIUS servers for authentication. • Tacacs. Users the list of all TRACACS servers for authentication.

Example: The following example sets authentication when accessing higher privilege levels.

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

6.10.2.1. no aaa authentication enable

Use this command to return to the default configuration.

Syntax	no aaa authentication enable {default | list-name}
Command Mode	Global Config

6.10.3. aaa authorization

Use this command to configure command authorization method lists. 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. If none is specified as the authorization method, command authorization is not applicable. A maximum of five authorization method lists can be created for the *commands* type.

Local method is not supported for command authorization. Command authorization with RADIUS will work if, and only if, the applied authentication method is also radius.

6.10.4. enable authentication

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

Syntax	enable authentication {default | list-name}
Command Mode	Line Config
<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.

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

```
(Routing) (Config)# line console
(Routing) (config-line)# enable authentication default
```

6.10.4.1. no enable authentication

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

Syntax	no enable authentication
Command Mode	Line Config

6.10.5. 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.

Syntax	aaa ias-user username user
Command Mode	Global Config

6.10.5.1. no aaa ias-user username

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

Syntax	no aaa ias-user username user
Command Mode	Global Config

Example: The following shows an example of the command.

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

6.10.6. 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
Syntax	aaa session-id [common | unique]
Command Mode	Global Config
<common>	Use the same session-id for all AAA Service types.
<unique>	Use a unique session-id for all AAA Service types.

6.10.6.1. no aaa session-id

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

Syntax	no aaa session-id [unique]
Command Mode	Global Config

6.10.7. 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 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.

Please 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 disable accounting.
- RADIUS is the only accounting method supported for DOT1X accounting.

Syntax	aaa accounting {exec | commands | dot1x} {default | list_name} {start-stop | stop-only |none} method1 [method2]
Command Mode	Global Config
<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 the radius server for accounting purposes.

Example: The following shows an example of the command.

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

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

```
(Routing) #
(Routing) #configure
```

```
(Routing) #aaa accounting exec ExecList stop-only tacacs
(Routing) #aaa accounting exec ExecList start-stop tacacs
(Routing) #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

6.10.7.1. no aaa accounting

This command deletes the accounting method list.

Syntax	no aaa accounting {exec | commands } {default | list_name default}
Command Mode	Global Config

Example: The following shows an example of the command.

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

6.10.8. 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 pre-encrypted.

Syntax	password [password] [encrypted]
Command Mode	AAA IAS User Config
<password>	Password for this level. Range: 8-64 characters
<encrypted>	Encrypted password to be entered, copied from another switch configuration.

6.10.8.1. no password (AAA IAS User Configuration)

Use this command to clear the password of a user.

Syntax	no password
Command Mode	AAA IAS User Config

Example: The following shows an example of the command.

```
(Routing) #
(Routing) #configure
(Routing) (Config)#aaa ias-user username user1
(Routing) (Config-aaa-ias-User)#password user123
```

```
(Routing) (Config-aaa-ias-User)#no password
```

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

```
(Routing) #
(Routing) #configure
(Routing) (Config)#aaa ias-user username 12fsdf213
(Routing) (Config-aaa-ias-User)#password 12fsdf213
(Routing) (Config-aaa-ias-User)#exit
(Routing) (Config)#
```

6.10.9. clear aaa ias-users

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

Syntax	clear aaa ias-users
Command Mode	Privileged Exec
<password>	Password for this level. Range: 8-64 characters
<encrypted>	Encrypted password to be entered, copied from another switch configuration.

Example: The following is an example of the command.

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

6.10.10. 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.

Syntax	show aaa ias-users [username]
Command Mode	Privileged EXEC

Example: The following is an example of the command.

```
(Routing) #
(Routing) #show aaa ias-users
UserName
------------
Client-1
Client-2
```

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

```
(Routing) #aaa ias-user username client-1
password a45c59xgh50s558d2b5cd40683cd458bac2c6c121d548537ad4c46104918f2c
encrypted exit
```

6.10.11. accounting

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

Syntax	accounting {exec | commands } {default | listname}
Command Mode	Line Configuration
<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.

Example: The following is a example of the command.

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

6.10.11.1. no accounting

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

Syntax	no accounting {exec|commands]
Command Mode	Line Configuration

6.10.12. show accounting

Use this command to display ordered methods for accounting lists.

Syntax	show accounting
Command Mode	Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(Routing) #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
```

6.10.13. show accounting methods

Use this command to display configured accounting method lists.

Syntax	show accounting methods
Command Mode	Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(Routing) #
(Routing) #show accounting methods
Acct Type  Method Name   Record Type  Method Type
---------- ------------  ------------ ------------
Exec       dfltExecList  start-stop   TACACS
Commands   dfltCmdsList  stop-only    TACACS
Commands   UserCmdAudit  start-stop   TACACS
DOT1X      dfltDot1xList start-stop   radius
```

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

6.10.14. 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**.

Syntax	login authentication {default | list-name}
Command Mode	Line Configuration
<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.

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

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

6.10.14.1. no login authentication

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

Syntax	no login authentication

Command Mode Line Configuration

6.11. User Account and Password Commands

6.11.1. 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.

Syntax	username name {password password [encrypted [override-complexity-check] | level level[encrypted [override-complexity-check]] | override-complexity-check]} | {level level [override-complexity-check] password}
Command 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). 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.

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

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

Example: The following example configures user test with password testPassword and assigns a user level of 1 (read-only). The password strength will not be validated.

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

Example: A third example.

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

Example: A fourth example.

```
(Routing) (Config)# username test password
e8d63677741431114f9e39a853a15e8fd35ad059e2e1b49816c243d7e08152b052eafb
f23b528d348cdba1b1b7ab91be84 2278e5e970dbfc62d16dcd13c0b864 level 1
encrypted override-complexity-check
(Routing) (Config)# username test level 15 password
Enter new password:********
Confirm new password:********
```

Example: A fifth example.

```
(Routing) (Config)# username test level 15 override-complexity-check
password
Enter new password:********
Confirm new password:********
```

6.11.1.1. no username

Use this command to remove a user name.

Syntax	no username name
Command Mode	Global Config

6.11.2. username name nopassword

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

Syntax	username name nopassword [level level]
Command Mode	Global Config
<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.

6.11.3. 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.

Syntax	username name unlock
Command Mode	Global Config

6.11.4. show users

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

Syntax	show users
Command Mode	Privileged EXEC
<User Name>	The name the user enters to login using the serial port or Telnet.
<User 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.

6.11.5. show users long

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

Syntax	show users long
Command Mode	Privileged EXEC

Example: The following shows an example of the command.

```
(Routing) #show users long
User Name
------------
admin
guest
test1111
```

6.11.6. show users accounts

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

Syntax	show users accounts [detail]
Command Mode	Privileged EXEC
<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:

<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.

Example: The following example displays information about the local user database.

```
(Routing) #show users accounts
UserName Privilege Password Password Lockout
Aging Expiry date
------------------ --------- -------- ------------ -------
admin 15 --- --- False
guest 1 --- --- False
(Routing) #show users accounts detail
UserName..................................... admin
Privilege.................................... 15
Password Aging............................... ---
Password Expiry.............................. ---
Lockout...................................... False
Override Complexity Check.................... Disable
Password Strength............................ ---
```

6.11.7. show users login-history

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

Syntax	show users login-history [name] [long]
Command Mode	Privileged EXEC
<name>	Name of the user. Range: 1-20 characters.

Example: The following example shows user login history outputs.

```
(Routing) #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
```

6.11.8. Password

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

Syntax	password cr
Command Mode	User EXEC

6.11.9. 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.

Syntax	password [password [encrypted]]
Command Mode	Line Config
<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.

Example: The following example specifies a password mcmxxyyy on a line.

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

Example: The following is another example of the command.

```
(Routing)(Config-line)# password testtest
(Routing) (Config-line)# password
e8d63677741431114f9e39a853a15e8fd35ad069f1g5e84616c243d7e08152b052eafbf2
3b528d348cdba1b1b7ab91be84 8568e5e970dhde62d16dcd13c0b864 encrypted
(Routing) (Config-line)# password
Enter new password:********
Confirm new password:********
```

6.11.9.1. no password (Line Configuration)

Use this command to remove the password on a line.

Syntax	no password
Command Mode	Line Config

6.11.10. 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.

Syntax	password
Command Mode	User EXEC

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

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

6.11.11. enable password

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

Syntax	enable password [password [encrypted]]
Command Mode	Privileged EXEC
<password>	Password string. Range: 8-64 characters.
<encrypted>	The encrypted password you entered, copied from another switch configuration. The encrypted password should be 128 characters long because the assumption is that the password is already encrypted with AES.

Example:The following shows an example of the command.

```
(Routing) #enable password testtest
(Routing) #enable password
e8d63677741431114f9e39a853a15e8fd35ad059e2e1b49816c243d7e08152b052eafbf2
3b528d348cdba1b1b7ab91be84 2278e5e970dbfc62d16dcd13c0b864 encrypted
(Routing) #enable password
Enter old password:********
Enter new password:********
Confirm new password:********
```

6.11.11.1. no enable password

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

Syntax	no enable password
Command Mode	Privileged EXEC

6.11.12. 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 0-64.

Default	8

Syntax	passwords min-length o-64
Command Mode	Global Config

6.11.12.1. no passwords min-length

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

Syntax	no passwords min-length
Command Mode	Global Config

6.11.13. 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
Syntax	passwords history 0-10
Command Mode	Global Config

6.11.13.1. no passwords history

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

Syntax	no passwords history
Command Mode	Global Config

6.11.14. passwords aging

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

Default	0
Syntax	passwords aging 1-365
Command Mode	Global Config

6.11.14.1. no passwords aging

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

Syntax	no passwords aging

Command Mode	Global Config

6.11.15. 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
Syntax	passwords lock-out 1-5
Command Mode	Global Config

6.11.15.1. no passwords lock-out

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

Syntax	no passwords lock-out
Command Mode	Global Config

6.11.16. 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
Syntax	passwords strength-check
Command Mode	Global Config

6.11.16.1. no passwords strength-check

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

Syntax	no passwords strength-check
Command Mode	Global Config

6.11.16.2. 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
Syntax	passwords maximum strength consecutive-characters 0-15
Command Mode	Global Config

6.11.16.3. 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
Syntax	passwords strength maximum consecutive-characters 0-15
Command Mode	Global Config

6.11.16.4. 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
Syntax	passwords strength minimum uppercase-letters
Command Mode	Global Config

6.11.16.5. no passwords strength minimum uppercase-letters

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

Syntax	no passwords minimum uppercase-letter
Command Mode	Global Config

6.11.16.6. 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
Syntax	passwords strength minimum lowercase-letters

Command Mode: Global Config

6.11.16.7. no passwords strength minimum lowercase-letters

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

Syntax	no passwords minimum lowercase-letter
Command Mode	Global Config

6.11.16.8. 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
Syntax	passwords strength minimum numeric-characters
Command Mode	Global Config

6.11.16.9. no passwords strength minimum numeric-characters

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

Syntax	no passwords minimum numeric-characters
Command Mode	Global Config

6.11.16.10. 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
Syntax	passwords strength minimum special-characters
Command Mode	Global Config

6.11.16.11. no passwords strength minimum special-characters

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

Syntax	no passwords minimum special-characters
Command Mode	Global Config

6.11.16.12. 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
Syntax	passwords strength minimum character-classes
Command Mode	Global Config

6.11.16.13. 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.

Syntax	no passwords minimum character-classes
Command Mode	Global Config

6.11.16.14. 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 insensitive and reverse) as a substring. The user can configure up to a maximum of 3 keywords.

Syntax	passwords strength exclude-keyword keyword
Command Mode	Global Config

6.11.16.15. no passwords strength exclude-keyword

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

Syntax	no passwords exclude-keyword [keyword]
Command Mode	Global Config

6.11.16.16. show passwords configuration

Use this command to display the configured password management settings.

Syntax	show passwords configuration
Command Mode	Privileged EXEC

Parameter	Definition
Minimum Password Length	Minimum number of characters required when changing passwords.

Parameter	Definition
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.

6.11.16.17. show passwords result

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

Syntax show passwords result

Command Mode Privileged EXEC

Parameter	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.

6.12. 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.

6.12.1. 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
Syntax	snmp-server {sysname name | location loc | contact con}
Command Mode	Global Config

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

6.12.2. 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.

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	Public and private, which you can rename. / Default values for remaining four community name are blank.
Syntax	snmp-server community community-string [{ro | rw | su }] [ipaddress ip-address] [view view-name]
Command Mode	Global Config

Parameter	Description
community-String	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-string can be up to 20 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

Parameter	Description
	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.

6.12.2.1. no snmp-server community

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

Syntax	no snmp-server community community-name
Command Mode	Global Config

6.12.3. snmp-server community-group

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

Syntax	snmp-server community-group community-stringgroup-name [ipaddress ipaddress]
Command Mode	Global Config
<community-string>	The community which is created and then associated with the group. Therange 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.

6.12.4. 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.

Default	disabled
Syntax	snmp-server enable traps violation
Command Mode	Global Config / Interface Config

6.12.4.1. no snmp-server enable traps violation

This command disables the sending of new violation traps.

Syntax	no snmp-server enable traps violation

Command Mode	Interface Config

6.12.5. snmp-server enable traps

This command enables the Authentication Flag.

Default	enabled
Syntax	snmp-server enable traps
Command Mode	Global Config

6.12.5.1. no snmp-server enable traps

This command disables the Authentication Flag.

Syntax	no snmp-server enable traps
Command Mode	Global Config

6.12.6. snmp-server enable traps bgp

The bgp option on the “snmp-server enable traps” command above enables the two traps defined in the standard BGP MIB, RFC 4273. Trap is sent when an adjacency reaches the ESTABLISHED state and when a backward adjacency state transition occurs.

Default	enabled
Syntax	snmp-server enable traps bgp state-changes limited
Command Mode	Global Config
<state-changes>	*limited* Enabled standard traps defined in RFC 4273.

6.12.7. snmp-server enable traps linkmode

This command may not be available on all platforms.

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.

Default	enabled
Syntax	snmp-server enable traps linkmode
Command Mode	Global Config

6.12.7.1. no snmp-server enable traps linkmode

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

Syntax	no snmp-server enable traps linkmode
Command Mode	Global Config

6.12.8. 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 into the terminal interface (EIA 232 or Telnet) and there is an existing terminal interface session.

Default	enabled
Syntax	snmp-server enable traps multiusers
Command Mode	Global Config

6.12.8.1. no snmp-server enable traps multiusers

This command disables Multiple User traps.

Syntax	no snmp-server enable traps multiusers
Command Mode	Global Config

6.12.9. snmp-server enable traps stpmode

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

Default	enabled
Syntax	snmp-server enable traps stpmode
Command Mode	Global Config

6.12.9.1. no snmp-server enable traps stpmode

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

Syntax	no snmp-server enable traps stpmode
Command Mode	Global Config

6.12.10. snmp-server enable traps trill

This command enables all TRILL SNMP traps.

Default	disable
Syntax	snmp-server enable traps trill
Command Mode	Global Config

6.12.10.1. no snmp-server enable traps trill

The no version of this command globally disables all TRILL SNMP traps.

Syntax	on snmp-server enable traps trill
Command Mode	Global Config

6.12.11. 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.
Syntax	snmp-server engineID local {engine-id|default}
Command Mode	Global Config
<engine-id>	A hexadecimal string identifying the engine-id. Engine-id must be an even length in the range of 6 to 32 hexadecimal characters.
<default>	Sets the engine-id to the default string, based on the device MAC address.

Changing the engineID will invalidate all SNMP configuration that exists on the box.

6.12.11.1. no snmp-server engineID local

This command removes the specified engine ID.

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

6.12.12. 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.
Syntax	snmp-server filter filtername oid-tree {included|excluded}
Command Mode	Global Config

<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).
<included>	The tree is included in the filter.
<excluded>	The tree is excluded from the filter.

6.12.12.1. no snmp-server filter

This command removes the specified filter.

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

6.12.13. snmp-server group

This command creates an SNMP access group.

Default	Generic groups are created for all versions and privileges using the default views.
Syntax	snmp-server group group-name {v1 | v2c | v3 {noauth | auth | priv}} [context context-name] [read read-view] [write write-view] [notify notify-view]
Command 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 SNMPv2c.
v2	The tree is included in the filter.
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.
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.

Parameter	Description
notify-view	The view this group will use when sending out traps. The range is 1 to 30 characters.

6.12.13.1. no snmp-server group

This command removes the specified group.

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

6.12.14. snmp-server host

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

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

Parameter	Description
host-addr	The IPv4 or IPv6 address of the host to send the trap or inform to.
community-string	Community string sent as part of the notification. The range is 1 to 20 characters.
traps	Send SNMP traps to the host. This option is selected by default.
version 1	The tree is included in the filter.
version 2c	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 acknowledgment 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.
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.

6.12.14.1. no snmp-server host

This command removes the specified host entry.

Syntax	no snmp-server host host-addr {traps|informs} version (1 | 2}
Command Mode	Global Config

6.12.15. snmp-server user

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

Default	No default users are created.
Syntax	snmp-server user usernamegroupname [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]
Command Mode	Global Config

Parameter	Description
username	The username the SNMPv3 user will connect to the switch as. 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.
version 2c	Sends SNMPv2c traps. This option is not available if informs is selected. This option is selected by default.
sha-key	A pregenerated SHA authentication key. The length is 40 characters.
des-key	A pregenerated DES encryption key. The length is 32 characters if MD5 is selected, 48 characters if SHA is selected.

6.12.15.1. no snmp-server user

This command removes the specified SNMPv3 user.

Syntax	no snmp-server user username
Command Mode	Global Config

6.12.16. snmp-server view

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

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

<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.

6.12.16.1. no snmp-server view

This command removes the specified view.

Syntax	no snmp-server view viewname [oid-tree]
Command Mode	Global Config

6.12.17. snmp-server v3-host

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

Default	No default hosts are configured.
Syntax	snmp-server v3-host host-addr username [traps | informs [timeout seconds] [retriesretries]] [auth | noauth | priv] [udpport port] [filter filtername]
Command Mode	Global Config
<host-addr>	The IPv4 or IPv6 address of the host to send the trap or inform to.
<user-name>	The 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>	The number of seconds to wait for an acknowledgment 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.
<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.

6.12.18. snmptrap source-interface

Use this command in Global Configuration mode to configure the global source-interface (Source IP address) for all SNMP communication between the SNMP client and the server.

Syntax	snmptrap source-interface {slot/port | loopback loopback-id|tunnel tunnel-id|vlan vlan-id}
Command Mode	Global Config
<slot/port>	Specifies the port to use as the source interface.
<loopback-id>	Specifies the loopback interface to use as the source interface. The range of the loopback ID is 0 to 7.
<tunnel-id>	Specifies the tunnel interface to use as the source interface. The range of the tunnel ID is 0 to 7.
<vlan-id>	Specifies the VLAN to use as the source interface.

6.12.18.1. no snmptrap source-interface

Use this command in Global Configuration mode to remove the global source-interface (Source IP selection) for all SNMP communication between the SNMP client and the server.

Syntax	no snmptrap source-interface
Command Mode	Global Config

6.12.19. show snmp

This command displays the current SNMP configuration.

Syntax	show snmp
Command Mode	Global Config

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
	GroupName	The group this community is assigned to.
	IPAddress	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.

6.12.20. show snmp engineID

This command displays the currently configured SNMP engineID.

Syntax	show snmp engineID
Command Mode	Privileged EXEC
<Local SNMP EngineID>	The current configuration of the displayed SNMP engineID.

6.12.21. show snmp filters

This command displays the configured filters used when sending traps.

Syntax	show snmp filters [filtername]
Command 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.

6.12.22. show snmp group

This command displays the configured groups.

Syntax	show snmp group [groupname]
Command 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.

6.12.23. show snmp user

This command displays the currently configured SNMPv3 users.

Syntax show snmp user [username]

Command 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.

6.12.24. show snmp views

This command displays the currently configured views.

Syntax show snmp views [viewname]

Command Mode Privileged EXEC

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

6.12.25. show trapflags

This command displays trap conditions. The command 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.

Syntax	show trapflags
Command Mode	Privileged EXEC

Parameter	Description
AuthenticationFlag	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.
BGP4 Traps	Can be enabled or disabled. The factory default is disabled. Indicates whether BGP4 traps are sent. (This field appears only on systems with the BGPv4 software package installed.)
OSPFv2 Traps	Can be enabled or disabled. The factory default is disabled. Indicates whether OSPF traps are sent. If any of the OSPF trap flags are not enabled, then the command displays disabled. Otherwise, the command shows all the enabled OSPF traps information.

6.12.26. show snmptrap source-interface

Use the **show snmptrap source-interface** command in Global Config mode to display the configured global source interface details used for an SNMP client. The IP address of the selected interface is used as source IP for all communications with the server.

Syntax	show snmptrap source-interface
Command Mode	Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(Config)# show snmptrap source-interface
SNMP Client Source Interface : 0/2
SNMP Client Source IPv4 Address : 192.168.2.20 [UP]
```

6.13. 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.

6.13.1. authorization network radius

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

Default	disable
Syntax	authorization network radius
Command Mode	Global Config

6.13.1.1. no authorization network radius

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

Syntax	no authorization network radius
Command Mode	Global Config

6.13.2. radius accounting mode

This command is used to enable the RADIUS accounting function.

Default	disabled
Syntax	radius accounting mode
Command Mode	Global Config

6.13.2.1. 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.

Syntax	no radius accounting mode
Command Mode	Global Config

6.13.3. 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.

Syntax	radius server attribute 4 [ipaddr]
Command Mode	Global Config
<4>	NAS-IP-Address attribute to be used in RADIUS requests.
<ipaddr>	The IP address of the server.

6.13.3.1. 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.

Syntax	no radius server attribute 4 [ipaddr]
Command Mode	Global Config

Example: The following shows an example of the command.

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

6.13.4. 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 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.

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

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, it must be removed from the configuration using the no form of the command before this command succeeds. 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 value in the range 0 - 65535, with 1813 being the default.

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

Syntax	radius server host {auth | acct} {ipaddr|dnsname} [name servername] [port 0-65535]
Command Mode	Global Config
<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.
<servername>	The alias name to identify the server.

6.13.4.1. 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.

Syntax	no radius server host {auth | acct} {ipaddr|dnsname}
Command Mode	Global Config

Example: The following shows an example of the command.

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

6.13.5. 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 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** command display, these secret keys are displayed in encrypted format. You cannot show these keys in plain text format.

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

Syntax	radius server key {auth | acct} {ipaddr|dnsname} encrypted password
Command Mode	Global Config
<ipaddr>	The IP address of the server.
<dnsname>	The DNS name of the server.
<password>	The password in encrypted format

Example: The following shows an example of the CLI command.

```
(Routing) (Config)#radius server key acct 10.240.4.10 encrypted
encrypt-string
```

6.13.6. radius server msgauth

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

Syntax	radius server msgauth ipaddr|dnsname
Command Mode	Global Config
<ipaddr>	The IP address of the server.
<dnsname>	The DNS name of the server.

6.13.6.1. no radius server msgauth

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

Syntax	no radius server msgauth ipaddr|dnsname
Command Mode	Global Config

6.13.7. 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.

Syntax	radius server primary {ipaddr|dnsname}

Command Mode	Global Config
<ipaddr>	The IP address of the server.
<dnsname>	The DNS name of the server.

6.13.8. 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 fallback 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
Command Mode	radius server retransmit retries
Command Mode	Global Config
<retries>	The maximum number of transmission attempts in the range of 1 to 15.

6.13.8.1. no radius server retransmit

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

Syntax	no radius server retransmit
Command Mode	Global Config

6.13.9. radius source-interface

Use this command to specify the physical or logical interface to use as the RADIUS client source interface (Source IP address). If configured, the address of source Interface is used for all RADIUS communications between the RADIUS server and the RADIUS client. The selected source-interface IP address is used for filling the IP header of RADIUS management protocol packets. This allows security devices (firewalls) to identify the source packets coming from the specific switch.

If a source-interface is not specified, the primary IP address of the originating (outbound) interface is used as the source address. If the configured interface is down, the RADIUS client falls back to its default behavior.

Syntax	radius source-interface {slot/port | loopback loopback-id | vlan vlan-id}
Command Mode	Global Config
<slot/port>	Specifies the port to use as the source interface.
<loopback-id>	Specifies the loopback interface to use as the source interface. The range of the loopback
<vlan-id>	Specifies the VLAN to use as the source interface.

6.13.9.1. no radius source-interface

Use this command to reset the RADIUS source interface to the default settings.

Syntax	no radius source-interface
Command Mode	Global Config

6.13.10. 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
Syntax	radius server timeout seconds
Command Mode	Global Config
<retries>	Maximum number of transmission attempts in the range 1-30

6.13.10.1. no radius server timeout

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

Syntax	no radius server timeout
Command Mode	Global Config

6.13.11. show radius

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

Syntax	show radius
Command Mode	Privileged EXEC

Parameter	Definition
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.
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.

Parameter	Definition
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 the accounting mode for all the servers is enabled or not.
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 the NAS-IP-Address attribute to be used in RADIUS requests.

Example: The following shows example CLI display output for the command.

```
(Routing) #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
```

6.13.12. show radius servers

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

Syntax	show radius servers [{ipaddr|dnsname | name [servername]}]
Command Mode	Privileged EXEC

Parameter	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.

Parameter	Description
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.
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.

Example: The following shows example CLI display output for the command.

```
(Routing) #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
(Routing) #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
```

```
(Routing) #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
```

```
(Routing) #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
```

6.13.13. show radius accounting

This command displays a summary of configured RADIUS accounting servers.

Syntax	show radius accounting name [servername]
Command Mode	Privileged EXEC

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

Example: The following shows example CLI display output for the command.

```
(Routing) #show radius accounting name
Host Address            Server Name          Port SecretConfigured
---------------------- ------------------------------- --------
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
```

```
(Routing) #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
```

6.13.14. show radius accounting statistics

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

Syntax	show radius accounting statistics {ipaddr|dnsname | name servername}

Command Mode Privileged EXEC

Parameter	Definition
ipaddr	The IP address of the server.
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 has not yet timed out or received a response.
Timeouts	The number of accounting timeouts to this server.
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.

Example: The following shows example CLI display output for the command.

```
(Routing) #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
```

```
(Routing) #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
```

6.13.15. show radius source-interface

Use the show radius source-interface command in Global Config mode to display the configured global source interface details used for a RADIUS client. The IP address of the selected interface is used as source IP for all communications with the server.

Syntax	show radius source-interface
Command Mode	Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(Routing) #show radius source-interface
RADIUS Client Source Interface............... 0/2
RADIUS Client Source IPv4 Address............ 192.168.2.20 [Up]
```

6.13.16. show radius statistics

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

Syntax	show radius statistics {ipaddr|dnsname | name servername}
Command Mode	Privileged EXEC

Parameter	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.

Parameter	Definition
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.
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.

Example: The following shows example CLI display output for the command.

```
(Routing) #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
```

```
(Routing) #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
```

6.14. 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.

6.14.1. 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.

Syntax	tacacs-server host ip-address|hostname
Command Mode	Global Config

6.14.1.1. 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.

Syntax	no tacacs-server host ip-address|hostname
Command Mode	Global Config

6.14.2. 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. The text-based configuration supports TACACS server 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** command display, these secret keys are displayed in encrypted format. You cannot show these keys in plain text format.

Syntax	tacacs-server key [key-string | encrypted key-string]
Command Mode	Global Config

6.14.2.1. 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.

Syntax	no tacacs-server key key-string
Command Mode	Global Config

6.14.3. 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.

Syntax	tacacs-server keystring
Command Mode	Global Config

Example: The following shows an example of the CLI command.

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

6.14.4. 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.

Default	5
Syntax	tacacs-server timeout timeout
Command Mode	Global Config

6.14.4.1. no tacacs-server timeout

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

Syntax	no tacacs-server timeout
Command Mode	Global Config

6.14.5. 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 (characters). The text-based configuration supports TACACS server 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** command display, these secret keys are displayed in encrypted format. You cannot show these keys in plain text format.

Syntax	key [key-string | encrypted key-string]
Command Mode	TACACS Config

6.14.6. 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.

Syntax	keystring
Command Mode	TACACS Config

Example: The following shows an example of the command.

```
(Routing) (Config)#tacacs-server host 1.1.1.1
(Routing) (Tacacs)#keystring
Enter tacacs key:********
Re-enter tacacs key:********
```

6.14.7. 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
Syntax	port port-number
Command Mode	TACACS Config

6.14.8. priority

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
Syntax	priority priority
Command Mode	TACACS Config

6.14.9. tacacs-server source-interface

Use this command in Global Configuration mode to configure the source interface (Source IP address) for TACACS+ server configuration. The selected source-interface IP address is used for filling the IP header of management protocol packets. This allows security devices (firewalls) to identify the source packets coming from the particular switch. If a source-interface is not specified, the primary IP address of the originating (outbound) interface is used as the source address.

Syntax	tacacs-server source-interface {slot/port | loopback loopback-id|vlan vlan-id}
Command Mode	Global Config
<slot/port>	Specifies the port to use as the source interface.
<loopback-id>	Specifies the loopback interface to use as the source interface. The range of the loopback ID is 0 to 7.
<vlan-id>	Specifies the VLAN to use as the source interface.

Example: The following shows an example of the command.

```
(Config)#tacacs-server source-interface loopback 0
(Config)#tacacs-server source-interface 0/1
(Config)#no tacacs-server source-interface
```

6.14.9.1. no tacacs-server source-interface

Use this command in Global Configuration mode to remove the global source interface (Source IP selection) for all TACACS+ communications between the TACACS+ client and the server.

Syntax	no tacacs-server source-interface
Command Mode	Global Config

6.14.10. 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.

Syntax	timeout timeout
Command Mode	TACACS Config

6.14.11. show tacacs

Use the show tacacs command to display the configuration and statistics of a TACACS+ server.

Syntax	show tacacs [ip-address|hostname]
Command Mode	Privileged EXEC

<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.

6.14.12. show tacacs source-interface

Use the **show tacacs source-interface** command in Global Config mode to display the configured global source interface details used for a TACACS+ client. The IP address of the selected interface is used as source IP for all communications with the server.

Syntax	show tacacs source-interface
Command Mode	Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(Routing) #show tacacs source-interface
TACACS Client Source Interface.................. 0/2
TACACS Client Source IPv4 Address.............. 192.168.2.20 [Up]
```

6.15. Configuration Scripting Commands

Configuration Scripting allows you to generate text-formatted script files representing the current configuration of a system. You can upload this 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 to capture the running configuration into a script. Use the copy command to transfer the configuration script to or from the switch.

Use the **show {startup-config | backup-config | factory-defaults}** command to view the configuration stored in the startup-config, backup-config, or factory-defaults file.

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:

1. The file extension must be “.scr”.
2. A maximum of ten scripts are allowed on the switch.
3. The combined size of all script files on the switch shall not exceed 2048 KB.
4. 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 by the parser.

The following lines show an example of a script:

```
! Script file for displaying management access
! Displays the information about remote connections
show telnet
! Display information about direct connections
show serial
! End of the script file!
```

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
```

6.15.1. script apply

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

Syntax	script apply scriptname
Command Mode	Privileged EXEC

6.15.2. 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.

Syntax	script delete {scriptname | all}
Command Mode	Privileged EXEC

6.15.3. script list

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

Syntax	script list
Command Mode	Global Config

Parameter	Definition
Configuration Script	Name of the script
Size	The size of the script file.

6.15.4. script show

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

Syntax	script show scriptname
Command Mode	Privileged EXEC

Parameter	Definition
Output Format	line number: line contents

6.15.5. 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.

Syntax	script validate scriptname
Command Mode	Privileged EXEC

6.16. Pre-login Banner, System Prompt, and Host Name Commands

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

6.16.1. 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 TFTP, SFTP, SCP, or Xmodem.

Default	none
Syntax	copy <tftp://<ipaddr>/<filepath>/<filename>> nvram:clibanner :: copy nvram:clibanner <tftp://<ipaddr>/<filepath>/<filename>>
Command Mode	Privileged EXEC

6.16.2. set prompt

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

Syntax	set prompt prompt_string
Command Mode	Privileged EXEC

6.16.3. set clibanner

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

Syntax	set clibanner line
Command Mode	Global Config
<line>	Banner text where “”(double quote) is a delimiting character. The banner message can be up to 2000 characters.

6.16.4. no set clibanner

Use this command to unconfigure the pre-login CLI banner.

Syntax	no set clibanner
Command Mode	Global Config

6.16.5. show clibanner

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

Default	No contents to display before displaying the login prompt.
Syntax	show clibanner
Command Mode	Privileged Exec

Example: The following shows example CLI display output for the command.

```
(Routing) #show clibanner
Banner Message configured :
==========================
--------------------------
TEST
```

6.16.6. hostname

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

Syntax	hostname hostname
Command Mode	Privileged Exec

Chapter 7. Utility Commands

This section describes the following utility commands available in the Fastpath CLI:

The commands in this section are in one of five functional groups:

- Show commands display switch settings, statistics, and other information.
- Configuration commands configure feathers and options of the switch. For every configuration command, there is a show command that displays the configuration setting.

- Copy commands transfer or save the configuration and informational files to and from the switch.
- Debug commands provide diagnostic information and help troubleshoot network issues.
- Clear commands clear some or all of the settings to factory defaults.

7.1. 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 when the switch is booted with no saved configuration found.
- 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 files 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.

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.

7.1.1. 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
Syntax	boot autoinstall {start |stop}
Command Mode	Privileged EXEC

7.1.2. boot host retrycount

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

Default	3

Syntax	boot host retrycount 1-3
Command Mode	Privileged EXEC

7.1.2.1. no boot host retrycount

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

Syntax	no boot host retrycount
Command Mode	Privileged EXEC

7.1.3. 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
Syntax	boot host dhcp
Command Mode	Privileged EXEC

7.1.3.1. no boot host dhcp

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

Syntax	no boot host dhcp
Command Mode	Privileged EXEC

7.1.4. 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
Syntax	boot host autosave
Command Mode	Privileged EXEC

7.1.5. no boot host autosave

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

Syntax	no boot host autosave
Command Mode	Privileged EXEC

7.1.6. 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
Syntax	boot host autoreboot
Command Mode	Privileged EXEC

7.1.6.1. no boot host autoreboot

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

Syntax	no boot host autoreboot
Command Mode	Privileged EXEC

7.1.7. erase startup-config

Use this command to erase the configuration file *startup-config*, 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.

Syntax	erase startup-config
Command Mode	Privileged EXEC

7.1.8. erase factory-defaults

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

Default	Disable
Syntax	erase factory-defaults
Command Mode	Global Config

7.1.9. show autoinstall

This command displays the current status of the AutoInstall process

Syntax	show autoinstall
Command Mode	Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(Routing) #show autoinstall
AutoInstall Mode.............................. Stopped
AutoInstall Persistent Mode................... Disabled
AutoSave Mode................................. Disabled
AutoReboot Mode............................... Enabled
AutoInstall Retry Count....................... 3
```

7.2. CLI Output Filtering Commands

7.2.1. 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.

Example: The following shows an example of the CLI command.

```
(Routing) #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
```

7.2.2. 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.

Example: The following shows example of the CLI command.

```
(Routing) #show running-config | include "spanning-tree" exclude
"configuration"
spanning-tree bpduguard
spanning-tree bpdufilter default
spanning-tree forceversion 802.1w
```

7.2.3. 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.

Example: The following shows an example of the CLI command.

```
(Routing) #show interface 0/1
Packets Received Without Error..................... 0
Packets Received With Error........................ 0
Broadcast Packets Received......................... 0
Packets Transmitted Without Errors................. 0
Transmit Packet Errors............................. 0
Collision Frames................................... 0
Time Since Counters Last Cleared................... 20 day 21 hr 30 min 9 sec
```

```
(Routing) #show interface 0/1 | exclude “Packets”
Transmit Packet Errors............................. 0
Collision Frames................................... 0
Time Since Counters Last Cleared................... 20 day 21 hr 30 min 9 sec
```

7.2.4. 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.

Example: The following shows an example of the CLI command.

```
(Routing) #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
(Routing) #
```

7.2.5. 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”).

Example: The following shows an example of the CLI command.

```
(Routing) #show running-config | section “inerface 0/1”
interface 0/1
no spanning-tree port mode
exit
```

7.2.6. show xxx|section “string1” “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.

7.2.7. show xxx|section “string1” 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.

7.3. Dual Image Commands

These commands are only available on selected Linux-based platforms.

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.

7.3.1. delete

This command deletes the backup image file from the permanent storage.

Syntax	delete backup
Command Mode	Privileged EXEC

7.3.2. 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.

Syntax	boot system {active | backup}
Command Mode	Privileged EXEC

7.3.3. 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.

Syntax	show bootvar
Command Mode	Privileged EXEC

7.3.4. filedescr

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

Syntax	filedescr {active | backup} text-description

Command Mode	Privileged EXEC

7.3.5. update bootcode

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

Syntax	update bootcode
Command Mode	Privileged EXEC

7.4. System Information and Statistics Commands

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

7.4.1. show arp switch

This command displays the contents of the IP stacklearns ARP entries associated with the management interfaces - network or service ports. ARP entries associated with routing interfaces are not listed.

Syntax	show arp switch
Command Mode	Privileged EXEC

Parameter	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 unit/slot/port of the physical interface.

7.4.2. dir

Use this command to list the files in the directory /mnt/fastpath in flash from the CLI.

Syntax	dir
Command Mode	Privileged EXEC

Example:

```
(Routing) #dir
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
```

7.4.3. 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.

Syntax	show eventlog
Command Mode	Privileged EXEC

Parameter	Definition
File	The file in which the event originated
Line	The line number of the event.
Task Id	The task ID of the event.
Code	The event code.
Time	The time this event occurred.

7.4.4. environment temprange

Use this command to set the allowed temperature range for normal operation.

Syntax	environment temprange min -100-100 max -100-100
Command Mode	Global Config
<min>	Sets the minimum allowed temperature for normal operation. The range is between -100C and 100C.The default is 0C.
<max>	Sets the maximum allowed temperature for normal operation. The range is between -100C and 100C.The default is 0C.

7.4.5. environment trap

Use this command to configure environment status traps.

Syntax	environment trap {fan|powersupply|temperature}
Command Mode	Global Config
<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.

7.4.6. show version

This command displays inventory information for the switch.

The show version command will replace the show hardwarecommand in future releases of the software.

Syntax show version

Command Mode Privileged EXEC

Parameter	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.
FRU Number	The field replaceable unit number.
Part Number	Manufacturing part number.
Maintenance Level	Hardware changes that are significant to software.
Manufacturer	Manufacturer descriptor field.
Software Version	The release.version.revision number of the code currently running on the switch.
Operating System	The operating system currently running on the switch.
Burned in MAC Address	Universally assigned network address.
Network Processing Device	The type of the processor microcode.
Additional Packages	The additional packages incorporate into this system

7.4.7. show platform vpd

This command displays vital product data for the switch.

Syntax show platform vpd

Command Mode Privileged EXEC / User EXEC

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.

Term	Definition
Timestamp	Timestamp at which the image is built

Example: The following shows example CLI display output for the command.

```
(Routing) #show platform vpd
Operational Code Image File Name.............. FastPath-Fastpath-esw-xgs4-
gto-BL20R-CS-6IQHr3v7m14b35
Software Version.............................. 3.7.14.35
Timestamp..................................... Thu Mar 7 14:36:14 IST
2013
```

7.4.8. show interface

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

Syntax	show interface {unit/slot/port | switchport | lag lag-id}
Command Mode	Privileged EXEC

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

Parameter	Definition
Packets Received Without Error	The total number of packets (including broadcast 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.
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 interface.
Transmit Packets Discarded	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent them 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.
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” as follows:

Parameter	Definition
Broadcast Packets Received	The total number of packets received that were directed to the broadcast address.
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.
Transmit Packet Errors	The number of outbound packets that could not be transmitted because of errors.
Address Entries Currently In Use	The total number of Forwarding Database Address Table entries now active on the switch, including learned and static entries.
VLAN Entries Currently In Use	The number of VLAN entries presently occupying the VLAN table.
Time Since Counters Last Cleared	The elapsed time, in days, hours, minutes, and seconds since the statistics for this switch were last cleared.

7.4.9. 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.

Syntax	show interfaces status [<interface>]
Command Mode	Privileged EXEC

7.4.10. show interface counters

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

Syntax	show interface counters
Command Mode	Privileged EXEC

Parameter	Definition
Port	The physical port, LAG, or CPU interface associated with the rest of the data in the row.
InOctets	The number of inbound octets received by the interface.
InUcastPkts	The number of inbound unicast packets received by the interface.
InMcastPkts	The number of inbound multicast packets received by the interface.
InBcastPkts	The number of inbound broadcast packets received by the interface.
OutOctets	The number of outbound octets transmitted by the interface.
OutUcastPkts	The number of outbound unicast packets transmitted by the interface.
OutMcastPkts	The number of outbound multicast packets transmitted by the interface.
OutBcastPkts	The number of outbound broadcast packets transmitted by the interface.

7.4.11. show interface ethernet

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

Syntax show interface ethernet {unit/slot/port|all|switchport}

Command Mode Privileged EXEC

Parameter	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). **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).

Parameter	Definition
	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. **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). **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 1519-1522 Octets** - The total number of packets (including bad packets) received and transmitted that were between 1519 and 1522 octets in length inclusive (excluding framing bits but including FCS octets). **Packets RX and TX 1523-2047 Octets** - The total number of packets (including bad 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.

Parameter	Definition
	Packets RX and TX 2048-4095 Octets - The total number of packets (including bad packets) received and transmitted 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 (including bad packets) received and transmitted that were between 4096 and 9216 octets in length inclusive (excluding framing bits, but including FCS octets) and were otherwise well formed.
Packets Received Successfully	**Total Packets Received Without Errors** - The total number of packets received that were without errors. **Unicast Packets Received** - The total number of subnetwork-unicast packets delivered to a higher-layer protocol. **Broadcast Packets Received** - The total number of good packets received that were delivered to a higher-layer protocol.
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 Received with MAC Errors	**Total Packets Received With MAC Errors** - The number of inbound packets 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 20ms. The allowed range to detect jabber is between 20ms and 150ms. **Fragments/Undersize Received** - The total number of packets received that were lesser than 64 octets (excluding framing bits, but including FCS octets). **Alignment Errors** - The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with a non-integral number of octets. **Rx FCS Errors** - The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with an integral number of octets.

Parameter	Definition
	Overruns - The total number of frames discarded as this port was overloaded with incoming packets, and could not keep up with the inflow.
Received Packets Not Forwarded	**Total Received Packets Not Forwarded** - A count of valid frames received which were discarded (in other words, filtered) by the forwarding process. **Local Traffic Frames** - The total number of frames dropped in the forwarding process because the destination address was located off of this port. **802.3x Pause Frames Received** - A count of MAC Control frames received on this interface with an opcode indicating the PAUSE operation. This counter does not increment when the interface is operating in half-duplex mode. **Unacceptable Frame Type** - The number of frames discarded from this port due to being an unacceptable frame type. **Reserved Address Discards** - The number of frames discarded that are destined to an IEEE 802.1 reserved address and are not supported by the system. **Broadcast Storm Recovery** - The number of frames discarded that are destined for FF:FF:FF:FF:FF when Broadcast Storm Recovery is enabled. **CFI Discards** - The total number of frames discarded that have CFI bit set and the addresses in RIF are in non-canonical format. **Upstream Threshold** - The number of frames discarded due to lack of cell descriptors available for that packet's priority level.
Packets Transmitted (Octets)	**Total Packets Transmitted (Octets)** - The total number of octets of data (including those in bad packets) transmitted 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) transmitted that were 64 octets in length (excluding framing bits but including FCS octets). **Packets Transmitted65-127 Octets** - The total number of packets (including bad packets) transmitted that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets). **Packets Transmitted 128-255 Octets** - The total number of packets (including bad packets) transmitted that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).

Parameter	Definition
	Packets Transmitted 256-511 Octets - The total number of packets (including bad packets) transmitted that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets). **Packets Transmitted 512-1023 Octets** - The total number of packets (including badpackets) transmitted that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets). **Packets Transmitted 1024-1518 Octets** - The total number of packets (including badpackets) transmitted 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 1522 octets (excluding framing bits, but including FCS octets) and were otherwise well formed. **Max Frame Size** - The maximum size of the info (non-MAC)field that this port will receive or transmit.
Packets Transmitted Successfully	**Total Packets Transmitted Successfully** - The total number of packets transmitted by this port to its segment. **Unicast Packets Received** - The total number of packets that higher-layer protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent. **Broadcast Packets Received** - The total number of packets that higher-layer protocols requested be transmitted to a Broadcast address, including those that were discarded or not sent.
Transmitted 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. One possible reason for discarding such a packet could be to free up buffer space.
Transmitted Errors	**Total Transmit Errors** - The sum of Single, Multiple, and Excessive Collisions. **Tx FCS Errors** - The total number of packets transmitted that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with an integral number of octets. **Oversized** - The total number of frames that exceeded the max permitted frame size. This counter has a max increment rate of 815 counts per sec. at 10 Mb/s. **Underrun Errors** - The total number of frames discarded because the transmit FIFO buffer became empty during frame transmission.

Parameter	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.
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. **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.
Dot1x Statistics	**EAPOL Frames Transmitted** - The number of EAPOL frames of any type that have been transmitted by this authenticator. **EAPOL Frames Received** - The number of valid EAPOL frames of any type 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 *all* keyword, the following information appears:

Parameter	Definition
Total Octets Transmitted	The total number of octets of data (including those in bad packets) transmitted 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 command interval.
Total Octets Received	The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including Frame Check Sequence (FCS) octets). This object can be used as a reasonable estimate of Ethernet utilization. If greater precision is desired, the etherStatsPkts and etherStatsOctets objects should be sampled before and after a common interval. The result of this equation is the value utilization which is the percent utilization of the Ethernet segment on a scale of 0 to 100 percent.
Total Packets Transmitted Successfully	The number of frames that have been transmitted by this port to its segment.
Total Packets Received Without Error	The total number of packets received that were without errors.

If you use the *switchport* keyword, the following information appears:

Parameter	Definition
Octets Received	The total number of octets of data received by the processor (excluding framing bits)
Total Packets Received Without Error	The total number of packets (including broadcast packets) received by the processor.
Unicast Packets Received	The number of subnetwork-unicast packets delivered to a higher-layer protocol.
Broadcast Packets Received	The total number of packets received that were directed to the broadcast address.
Receive Packets Discarded	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent them being deliverable to a higher-layer protocol. A possible reason for discarding a packet could be to free up buffer space.
Octets Transmitted	The total number of octets transmitted out of the interface, including framing characters.
Packets Transmitted without Errors	The total number of packets transmitted out of the interface.
Unicast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
Broadcast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to a Broadcast address, including those that were discarded or not sent.

Parameter	Definition
Most Address Entries Ever Used	The highest number of Forwarding Database Address Table entries that have been learned by this switch since the most recent reboot.
Address Entries in Use	The number of Learned and static entries in the Forwarding Database Address Table for this switch.
Maximum VLAN Entries	The maximum number of Virtual LANs (VLANs) allowed on this switch.
Most VLAN Entries Ever Used	The largest number of VLANs that has been active on this switch since the last reboot.
Static VLAN Entries	The number of presently active VLAN entries on this switch that have been created statically.
VLAN Deletes	The number of VLANs on this switch that have been created and then deleted since the last reboot.
Time Since Counters Last Cleared	The elapsed time, in days, hours, minutes, and seconds, since the statistics for this switch were last cleared.

Example: The following shows example CLI display output for the command when you use the all keyword.

```
(Routing) #show interface ethernet all
Port  Bytes Tx Bytes Rx Packets Tx Packets Rx
----- -------- -------- ---------- ----------
0/1          0        0          0          0
0/2          0        0          0          0
..
..
1/1          0        0          0          0
1/2          0        0          0          0
..
..
```

7.4.12. show interface ethernet switchport

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

Syntax	show interface ethernet interface-id switchport
Command Mode	Privileged EXEC
<interface-id>	The unit/slot/port of the switch.
<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.

7.4.13. 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 {unit/slot/port |laglag-id}* parameter to view MAC addresses on a specific interface. Use the *vlan vlan_id* parameter to display information about MAC addresses on a specified VLAN.

Syntax	show mac-addr-table [{ macaddr vlan_id| all | count | interface { unit/slot/port | lag lag-id} | vlan vlan_id}
Command Mode	Privileged EXEC

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

Parameter	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.
Interface	The port through which this address was learned.
Interface Index	This object indicates the if Index of the interface table entry associated with this port.
Status	The status of this entry. The meanings of the values are: Static, Learned, Management, Self, Other
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.

7.4.14. 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.

Syntax	process cpu threshold type total rising 1-100 interval
Command Mode	Global Config

Parameter	Definition
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).
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).

7.4.15. 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 *all* option.

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 script name is provided with a file name extension of redirected to a script file.

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.

If you use a text-based configuration file, the **show running-config** command will only display 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 a 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 trap flag 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*.

Syntax	show running-config [all | scriptname]
Command Mode	Privileged EXEC

7.4.16. show running-config interface

Use this command to display the running configuration for a specific interface. Valid interfaces include physical, LAG, loopback, tunnel and VLAN interfaces.

Syntax	show running-config interface { interface | lag { lag-intf-num } | loopback { loopback-id } | tunnel { tunnel-id } | vlan { vlan-id } }
Command Mode	Privileged EXEC

Parameter	Definition
interface	Running configuration for the specified interface.
lag-intf-num	Running configuration for the LAG interface.
loopback-id	Running configuration for the loopback interface.
tunnel-id	Running configuration for the tunnel interface.
vlan-id	Running configuration for the VLAN routing interface.

The following information is displayed for the command:

Parameter	Definition
unit/slot/port	Enter an interface in unit/slot/port format.

Parameter	Definition
lag	Display the running config for a specified lag interface.
loopback	Display the running config for a specified loopback interface.
tunnel	Display the running config for a specified tunnel interface.
vlan	Display the running config for a specified vlan routing interface.

Example: The following shows example CLI display output for the command.

```
(Routing) #show running-config interface 0/1
!Current Configuration:
!
interface 0/1
addport 3/1
exit
(Routing) #
```

7.4.17. 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 a flash. With this command, the files are decompressed while displaying their content.

Syntax	show { startup-config | backup-config | factory-defaults }
Command Mode	Privileged EXEC
<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.

Example: The following shows example CLI display output for the command using the startup-config parameter.

```
(Routing) #show startup-config
!Current Configuration:
!
!System Description "56854 Trident2 System - 48 TENGIG 6 FORTYGIG, 1.0.6,
Linux 2.6.34.6, active=image1"
!System Software Version "1.0.6"
!System Up Time "0 days 16 hrs 23 mins 5 secs"
!Cut-through mode is configured as disabled
!Additional Packages BGP-4,QOS,Multicast,IPv6,Routing,Data Center
!Current SNTP Synchronized Time: SNTP Client Mode Is Disabled
!
vlan database
vlan 10
```

```
exit
configure
line console
serial baudrate 115200
exit
line telnet
exit
line ssh
exit
!
interface 0/1
description 'intf1'
exit
router ospf
exit
ipv6 router ospf
exit
exit
```

Example: The following shows example CLI display output for the command using the backup-config parameter.

```
(Routing) #show backup-config
!Current Configuration:
!
!System Description "56854 Trident2 System - 48 TENGIG 6 FORTYGIG, 1.0.6,
Linux 2.6.34.6, active=image1"
!System Software Version "1.0.6"
!System Up Time "0 days 16 hrs 23 mins 5 secs"
!Cut-through mode is configured as disabled
!Additional Packages BGP-4,QOS,Multicast,IPv6,Routing,Data Center
!Current SNTP Synchronized Time: SNTP Client Mode Is Disabled
!
vlan database
vlan 10
exit
configure
line console
serial baudrate 115200
exit
line telnet
exit
line ssh
exit
!
interface 0/1
description 'intf1'
exit
router ospf
exit
ipv6 router ospf
exit
```

```
exit
```

Example: The following shows example CLI display output for the command using the factory-defaults parameter.

```
(Routing) #show factory-defaults
!Current Configuration:
!
!System Description "56854 Trident2 System - 48 TENGIG 6 FORTYGIG, 1.0.6,
Linux 2.6.34.6, active=image1"
!System Software Version "1.0.6"
!System Up Time "0 days 16 hrs 23 mins 5 secs"
!Cut-through mode is configured as disabled
!Additional Packages BGP-4,QOS,Multicast,IPv6,Routing,Data Center
!Current SNTP Synchronized Time: SNTP Client Mode Is Disabled
!
vlan database
vlan 10
exit
configure
line console
serial baudrate 115200
exit
line telnet
exit
line ssh
exit
!
interface 0/1
description 'intf1'
exit
router ospf
exit
ipv6 router ospf
exit
exit
```

7.4.18. show sysinfo

This command displays switch information.

Syntax	show sysinfo
Command Mode	Privileged EXEC

Parameter	Definition
Switch Description	Text used to identify this switch.
System Name	Name used to identify the switch. The factory default is blank.
System Location	Text used to identify the location of the switch. The factory default is blank.

Parameter	Definition
System Contact	Text used to identify a contact person for this switch. The factory default is blank.
System ObjectID	The base object ID for the switch.
System Up Time	The time in days, hours and minutes since the last switch reboot.
MIBs Supported	A list of MIBs supported by this agent.

7.4.19. show tech-support

Use the **show tech-support** command to display system and configuration information for the whole system, or for bgp, bgp-ipv6, ospf, or ospfv3 when you contact technical support. The output includes log history files from previous runs. 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 port all

show isdp neighbors

show logging

show eventlog

show logging buffered

show trap log

show previous run persistent logs

show running config

show debugging

The log messages are sorted and displayed in reverse chronological order.

Syntax	show tech-support [bgp|bgp-ipv6|ospf|ospfv3]
Command Mode	Privileged EXEC

7.4.20. 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.

Example: Length command on Line Console mode applies for Serial Console session.

Default	24
Syntax	length value
Command Mode	Line Config

7.4.20.1. no length value

Use this command to set the pagination length to the default value number of lines.

Syntax	no length value
Command Mode	Line Config

7.4.21. 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
Syntax	terminal length value
Command Mode	Privileged EXEC

7.4.21.1. 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.

Syntax	no terminal length value
Command Mode	Privileged EXEC

7.4.22. show terminal length

Use this command to display all the configured terminal length values.

Syntax	show terminal length
Command Mode	Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(Routing) #show terminal length
Terminal Length:
----------------------
For Current Session
For Serial Console……..24
```

```
For Telnet Sessions
For SSH Sessions……..24
```

7.4.23. memory free low-watermark processor

Use this command to get notifications when the CPU free memory falls below the configured threshold. 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.

Syntax	memory free low-watermark processor 1-1034956
Command Mode	Global Config
<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).

7.5. Logging Commands

7.5.1. logging buffered

This command enables logging to an in-memory log that keeps up to 128 logs.

Default	disabled; critical when enabled
Syntax	logging buffered
Command Mode	Global Config

7.5.1.1. no logging buffered

This command disables logging to in-memory log.

Syntax	no logging buffered
Command Mode	Global Config

7.5.2. 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
Syntax	logging buffered wrap
Command Mode	Global Config

7.5.2.1. no logging buffered wrap

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

Syntax	no logging buffered wrap
Command Mode	Global Config

7.5.3. 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.

Default	enabled
Syntax	logging cli-command
Command Mode	Global Config

7.5.3.1. no logging cli-command

This command disables the CLI command Logging feature.

Syntax	no logging cli-command
Command Mode	Global Config

7.5.4. logging console

This command enables logging to the console. You can specify the *severity level* 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
Syntax	logging console [severitylevel]
Command Mode	Global Config

7.5.4.1. no logging console

This command disables logging to the console.

Syntax	no logging console
Command Mode	Global Config

7.5.5. logging host

This command configures the logging host parameters. You can configure up to eight hosts.

Default	Port-514 Level-critical(2)
Syntax	logging host {hostaddress|hostname} addresstype {port severitylevel}
Command Mode	Global Config
<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).

7.5.6. logging host reconfigure

This command enables logging host reconfiguration.

Syntax	logging host reconfigure hostindex
Command Mode	Global Config
<hostindex>	Enter the Logging Host Index for which to change the IP address.

7.5.7. logging host remove

This command disables logging to host.

Syntax	logging host remove hostindex
Command Mode	Global Config

7.5.8. 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
Syntax	logging persistent severity level
Command Mode	Global Config

7.5.8.1. no logging persistent

Use this command to disable the persistent logging in the switch.

Syntax	no logging persistent
Command Mode	Global Config

7.5.9. logging port

This command sets the local port number of the LOG client for logging messages. The portid can be in the range from 1 to 65535.

Default	514
Syntax	logging port portid
Command Mode	Global Config

7.5.9.1. no logging port

This command resets the local logging port to the default.

Syntax	no logging port

Command Mode	Global Config

7.5.10. logging syslog

This command enables syslog logging.

Default	disabled
Syntax	logging syslog
Command Mode	Global Config

7.5.10.1. no logging syslog

This command disables syslog logging.

Syntax	no logging syslog
Command Mode	Global Config

7.5.11. logging syslog port

This command sets syslog logging port number. The portid parameter is an integer with a range of 1-65535.

Default	disabled
Syntax	logging syslog port portid
Command Mode	Global Config

7.5.11.1. no logging syslog port

This command sets syslog logging port number to the default value.The default value is 514.

Syntax	no logging syslog port
Command Mode	Global Config

7.5.12. logging syslog source-interface

Use this command to specify the physical or logical interface to use as the Syslog client source interface. If configured, the address of source Interface is used for all Syslog communications between the Syslog server and the Syslog client. Otherwise, there is no change in behavior. If the configured interface is down, the Syslog client falls back to normal behavior.

Syntax	logging syslog source-interface {unit/slot/port|{loopback loopback-id}|{tunnel tunnel-id}|{vlan vlan-id}

Command Mode	Global Config
<unit/slot/port>	Specifies the port to use as the source interface.
<loopback-id>	Specifies the loopback interface to use as the source interface. The range of the loopback ID is 0 to 7.
<tunnel-id>	Specifies the tunnel interface to use as the source interface. The range of the tunnel ID is 0 to 7.
<vlan-id>	Specifies the VLAN to use as the source interface.

7.5.12.1. no logging syslog source-interface

Use this command to remove the configured global source interface (Source IP selection) for all Syslog communications between the Syslog client and the server.

Syntax	no logging syslog source-interface
Command Mode	Global Config

7.5.13. show logging

This command displays logging configuration information.

Syntax	show logging
Command Mode	Privileged EXEC

Parameter	Definition
Logging Client Local Port	Port on the collector/relay to which syslog messages are sent.
Logging Client Source Interface	The interface configured as the source interface for the Syslog client.
Logging Client Source IPv4 Address	The IP address configured on the Syslog client source interface.
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 servity are logged.
Buffered Logging	Shows whether buffered logging is enabled.
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 Error	Number of messages that could not be processed due to error or lack of resources.

Parameter	Definition
Log Messages Relayed	Number of messages sent to the collector/relay.

7.5.14. show logging buffered

This command displays buffered logging (system startup and system operation logs).

Syntax show logging buffered

Command Mode Privileged EXEC

Parameter	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.

7.5.15. show logging hosts

This command displays all configured logging hosts.

Syntax show logging hosts

Command Mode Privileged EXEC

Parameter	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).

7.5.16. show logging persistent

Use the **show logging persistent** command to display persistent log entries. If *log-files* is specified, the persistent log files the system are displayed.

Syntax show logging persistent [log-files]

Command Mode Privileged EXEC

Parameter	Definition
Persistent Logging	If persistent logging is enabled or disabled.
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.

Example: 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
```

7.5.17. show logging traplogs

This command displays SNMP trap events and statistics.

Syntax show logging traplogs

Command Mode Privileged EXEC

Parameter	Definition
Number of Traps Since Last Reset	The number of traps since the last boot.
Trap Log Capacity	The number of persistent log entries.
Number of Traps Since Log Last Viewed	The number of new traps since the command was last executed.
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.

7.5.18. clear logging buffered

This command clears buffered logging (system startup and system operation logs).

Syntax clear logging buffered

Command Mode Privileged EXEC

7.6. Email Alerting and Mail Server Commands

7.6.1. 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 severity level 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
Syntax	logging email [severitylevel]
Command Mode	Global Config

7.6.1.1. no logging email

This command disables email alerting.

Syntax	no logging email
Command Mode	Global Config

7.6.2. logging email urgent

This command sets the lowest severity level at which log messages are e-mailed immediately in a single e-mail message. Specify the severity level 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.
Syntax	logging email urgent {severitylevel | none}
Command Mode	Global Config

7.6.3. no logging email urgent

This command resets the urgent severity level to the default value.

Syntax	no logging email urgent
Command Mode	Global Config

7.6.4. 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 [mailto:admin@yourcompany.com].

Syntax	logging email message-type {urgent |non-urgent |both} to-addr to-email-addr
Command Mode	Global Config

7.6.4.1. no logging email message-type to-addr

This command removes the configured to-addr field of email.

Syntax	no logging email message-type {urgent |non-urgent |both} to-addr to-email-addr
Command Mode	Global Config

7.6.5. logging email from-addr

This command configures the email address of the sender (the switch).

Default	switch@broadcom.com [mailto:switch@broadcom.com]
Syntax	logging email from-addr from-email-addr
Command Mode	Global Config

7.6.5.1. no logging email from-addr

This command removes the configured email source address.

Syntax	no logging email from-addr from-email-addr
Command Mode	Global Config

7.6.6. 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
Syntax	logging email message-type {urgent |non-urgent |both} subject subject
Command Mode	Global Config

7.6.6.1. 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.

Syntax	no logging email message-type {urgent |non-urgent |both} subject
Command Mode	Global Config

7.6.7. 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 minutes.

Default	30 minutes
Syntax	logging email logtime minutes
Command Mode	Global Config

7.6.7.1. no logging email logtime

This command resets the non-urgent log time to the default value.

Syntax	no logging email logtime
Command Mode	Global Config

7.6.8. 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.
Syntax	logging traps severitylevel
Command Mode	Global Config

7.6.8.1. no logging traps

This command resets the SNMP trap logging severity level to the default value.

Syntax	no logging traps
Command Mode	Global Config

7.6.9. logging email test message-type

This command sends an email to the SMTP server to test the email alerting function.

Syntax	logging email test message-type {urgent |non-urgent |both} message-body message-body
Command Mode	Global Config

7.6.10. show logging email config

This command displays information about the email alert configuration.

Syntax	show logging email config
Command Mode	Privileged EXEC

Parameter	Definition
Email Alert Logging	The administrative status of the feature: enabled or disabled
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 Addressable	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.

7.6.11. show logging email statistics

This command displays email alerting statistics.

Syntax	show logging email statistics

Command Mode Privileged EXEC

Parameter	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.

7.6.12. clear logging email statistics

This command resets the email alerting statistics.

Syntax clear logging email statistics

Command Mode Privileged EXEC

7.6.13. 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 or DNS name format.

Syntax mail-server {ip-address | hostname}

Command Mode Global Config

7.6.13.1. no mail-server

This command removes the specified SMTP server from the configuration.

Syntax no mail-server {ip-address | hostname}

Command Mode Global Config

7.6.14. 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

Syntax	security {tlsv1 | none}
Command Mode	Mail Server Config

7.6.15. 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 non-standard port in the range 1 to 65535 is also allowed.

Default	25
Syntax	port {465 | 25 | 1?5535}
Command Mode	Mail Server Config

7.6.16. username (Mail Server Config)

This command configures the login ID the switch uses to authenticate with the SMTP server.

Default	admin
Syntax	username name
Command Mode	Mail Server Config

7.6.17. password

This command configures the password the switch uses to authenticate with the SMTP server.

Default	admin
Syntax	password password
Command Mode	Mail Server Config

7.6.18. show mail-server config

This command displays information about the email alert configuration.

Syntax	show mail-server {ip-address | hostname | all} config
Command Mode	Privileged EXEC

Parameter	Definition
No of mail servers configured	The number of SMTP servers configured on the switch.
Email Alert Mail Server Address	The IPv4 address or DNS hostname of the configured SMTP server.

Parameter	Definition
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.

7.7. System Utility and Clear Commands

7.7.1. clear config

This command resets the configuration of the switch to the configuration present in the *factory-defaults* configuration file, if this file is present, without powering off the switch. If the *factory-defaults* configuration file is not present, then Fastpath-compile time defaults are applied to 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.

Syntax	clear config
Command Mode	Privileged EXEC

7.7.2. clear counters

This command clears the statistics for a specified unit/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.

Syntax	clear counters {unit/slot/port | all [vrf vrf-name] }
Command Mode	Privileged EXEC

7.7.3. 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.

Syntax	clear pass
Command Mode	Privileged EXEC

7.7.4. clear traplog

This command clears the trap log.

Syntax	clear traplog
Command Mode	Privileged EXEC

7.7.5. clear vlan

This command resets VLAN configuration parameters to the factory defaults.

Syntax	clear vlan

Command Mode	Privileged EXEC

7.7.6. logout

This command closes the current telnet connection or resets the current serial connection.

Save configuration changes before logging out.

Syntax	logout
Command Mode	Privileged EXEC

7.7.7. ping

Use this command to determine whether another computer is on the network. Ping provides a synchronous response when initiated from the CLI interface.

For information about the ping command for IPv6 hosts, see “ping ipv6”.

Default	The default count is 1. / The default interval is 3seconds. / The default size is 0 bytes
Syntax	ping {ip-address| hostname | {ipv6 {interface {unit/unit/slot/port | vlan 1-4093 | loopback loopback-id | network | serviceport | tunnel tunnel-id } link-local-address} | ip6addr | hostname} [count count] [interval 1-60] [size size] [source ip-address | ip6addr | {unit/unit/slot/port | vlan 1-4093 | serviceport | network}]
Command Mode	Privileged EXEC

Using the options described below, you can specify the number and size of Echo Requests and the interval between Echo Requests.

Parameter	Definition
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.
size	Use the size parameter to specify the size, in bytes, of the payload of the Echo Requests sent. The range is 0 to 13000 bytes.
source	Use the source parameter to specify the source IP/IPv6 address or interface to use when sending the Echo requests packets.

Parameter	Definition
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
link-local-address	The link-local IPv6 address to ping over an interface.

Example: ping success:

```
(Routing) #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
```

Example: ping failure:

In Case of Unreachable Destination:

```
(Routing) # 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:

```
(Routing) # 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
```

7.7.8. 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.

Syntax quit

7.7.9. 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.

Syntax	reload [cr | unit]
Command Mode	Privileged EXEC
<cr>	Press enter to execute the command.
<unit>	Enter switch ID in the range of 1 to 6.

7.7.10. 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.

Syntax	copy source destination {verify | noverify}
Command Mode	Privileged EXEC

Replace the source and destination parameters with the options in the Table 7.1, “Source-destination table” table. For the **url** source or destination, use one of the following values:

{xmodem | *ymodem* | *zmodem* | *tftp://ipaddress*|*hostname/filepath/filename* | *ftp://user@ipaddr*| *hostname/path/filename;* | *scp://user@ipaddr*|*hostname/path/filename* | *sftp://user@ipaddr*| *hostname/path/filename* | *usb://filepath/filename}*

verify | *noverify* is only available if the image/configuration verify options feature is enabled. *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 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 [mailto:username@ipaddress]/filepath/filename} }

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.

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.

Syntax	copy [<mode/file>] nvram:{openflow-ssl-ca-cert | openflow-ssl-cert | openflow-ssl-priv-key}
Command Mode	Privileged EXEC

Remember to upload the existing fastpath.cfg file off the switch prior to loading a new release image in order to make a backup.

Table 7.1. Source-destination table

Source	Destination	Description
nvram: application:sourcefilename	url	Copies an application to the server.
nvram:backup-config	nvram:startup-config	Copies the backup configuration to the startup configuration.
nvram:clibanner	url	Copies the CLI banner to a server.
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 usb://filepath/filename	Uploads the core dump file on the local system to an external TFTP/FTP/SCP/SFTP server.
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.

Source	Destination	Description
nvram:startup-config	url	Copies the startup configuration to a server.
nvram:startup-log	url	Copies the startup log to a server
nvram:traplog	url	Copies the trap log file to a server.
system:image	url	Saves the running configuration to a server.
system:running-config	nvram:startup	Saves the running configuration to NVRAM.
system:running-config	nvram:factory	Saves the running configuration to NVRAM to the *factory-defaults* file.
url	nvram:application destfilename	Downloads an application to the system.
url	nvram:backup-config	Downloads the backup configuration to thesystem
url	nvram:clibanner	Downloads the CLI banner to the system.
url	nvram:fastpath.cfg	Downloads the binary config file to the system
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: (Routing) #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*
url	nvram:sshkey-rsa1	Downloads an SSH key file.
url	nvram:sshkey-rsa2	Downloads an SSH key file.
url	nvram:openflow-ssl-ca-cert	Downloads Openflow CA Certificate.
url	nvram:openflow-ssl-cert	Downloads Openflow Switch Certificate.

Source	Destination	Description
url	nvram:openflow-ssl-priv-key	Downloads Openflow Private Key.
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 userattributes available in the downloaded file.
url	{active / backup}	Download an image from the remote server to either image. In a stacking environment, the downloaded image is distributed to the stack nodes.
{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.
{active / backup}	unit://unit/{active /backup}	Copy an image from the management node to a given node in a Stack. Use the unit parameter to specify the node to which the image should be copied.
{active / backup}	unit://*/{active / backup}	Copy an image from the management node to all of the nodes in a Stack.

Example: The following shows an example of downloading and applying ias users file.

```
(Routing) #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.
(Routing) #
```

7.7.11. 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.

Syntax	write memory [confirm]
Command Mode	Privileged EXEC

7.8. 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).

7.8.1. 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
Syntax	sntp broadcast client poll-interval poll-interval
Command Mode	Global Config

7.8.1.1. no sntp broadcast client poll-interval

This command resets the poll interval for SNTP broadcast client back to the default value.

Syntax	no sntp broadcast client poll-interval
Command Mode	Global Config

7.8.2. 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
Syntax	sntp client mode [broadcast | unicast]
Command Mode	Global Config

7.8.2.1. no sntp client mode

This command disables Simple Network Time Protocol (SNTP) client mode.

Syntax	no sntp client mode
Command Mode	Global Config

7.8.3. sntp client port

This command sets the SNTP client port ID to a value from 1-65535. 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
Syntax	sntp client port portid
Command Mode	Global Config

7.8.3.1. no sntp client port

This command resets the SNTP client port back to its default value.

Syntax	no sntp client port
Command Mode	Global Config

7.8.4. 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
Syntax	sntp unicast client poll-interval [poll-interval]
Command Mode	Global Config

7.8.4.1. no sntp unicast client poll-interval

This command resets the poll interval for SNTP unicast clients to its default value.

Syntax	no sntp unicast client poll-interval
Command Mode	Global Config

7.8.5. sntp unicast client poll-timeout

This command will set the poll timeout for SNTP unicast clients in seconds to a value from 1-30.

Default	5
Syntax	sntp unicast client poll-timeout poll-timeout
Command Mode	Global Config

7.8.5.1. no sntp unicast client poll-timeout

This command will reset the poll timeout for SNTP unicast clients to its default value.

Syntax	no sntp unicast client poll-timeout
Command Mode	Global Config

7.8.6. 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
Syntax	sntp unicast client poll-retry poll-retry
Command Mode	Global Config

7.8.6.1. no sntp unicast client poll-retry

This command will reset the poll retry for SNTP unicast clients to its default value.

Syntax	no sntp unicast client poll-retry
Command Mode	Global Config

7.8.7. sntp server

This command configures an SNTP server (a maximum of three). The server address is an IPv4/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.

Syntax	sntp server {ipaddress | ipv6address | hostname} [priority [version [portid]]]
Command Mode	Global Config

7.8.7.1. no sntp server

This command deletes an server from the configured SNTP servers.

Syntax	no sntp server remove {ipaddress | ipv6address | hostname}
Command Mode	Global Config

7.8.8. sntp source-interface

Use this command to specify the physical or logical interface to use as the SNTP client source interface. If configured, the address of source Interface is used for all SNTP communications between the SNTP server and the SNTP client. Otherwise there is no change in behavior. If the configured interface is down, the SNTP client falls back to its default behavior.

Syntax	sntp source-interface {unit/slot/port | loopback loopback-id | tunnel tunnel-id | vlan vlan-id}
Command Mode	Global Config
<unit/slot/port>	Specifies the port to use as the source interface.

<loopback-id>	Specifies the loopback interface to use as the source interface. The range of the loopback ID is 0 to 7.
<tunnel-id>	Specifies the tunnel interface to use as the source interface. The range of the tunnel ID is 0 to 7.
<vlan-id>	Specifies the VLAN to use as the source interface.

7.8.8.1. no sntp source-interface

Use this command to reset the SNTP source interface to the default settings.

Syntax	no sntp source-interface
Command Mode	Global Config

7.8.9. show sntp

This command is used to display SNTP settings and status.

Syntax	show sntp
Command Mode	Privileged EXEC

Parameter	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)
Broadcast Count	Current number of unsolicited broadcast messages that have been received and processed by the SNTP client since last reboot.

7.8.10. show sntp client

This command is used to display SNTP client settings.

Syntax	show sntp client
Command Mode	Privileged EXEC

Parameter	Definition
Client Supported Modes	Supported SNTP Modes (Broadcast, Unicast).
SNTP Version	The highest SNTP version the client supports.
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

Parameter	Definition
	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.

7.8.11. show sntp server

This command is used to display SNTP server settings and configured servers.

Syntax show sntp server

Command Mode Privileged EXEC

Parameter	Definition
Server IP Address / Hostname	IP address or hostname of configured SNTP Server.
Server Type	Address type of server (IPv4 or 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:

Parameter	Definition
IP Address / Hostname	IP address or hostname of configured SNTP Server.
Address Type	Address Type of configured SNTP server (IPv4 or 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.

7.8.12. show sntp source-interface

Use this command to display the SNTP client source interface configured on the switch.

Syntax	show sntp source-interface
Command Mode	Privileged EXEC

Parameter	Definition
SNTP Client Source Interface	The interface ID of the physical or logical interface configured as the SNTP client source interface.
SNTP Client Source IPv4 Address	Address type of server (IPv4 or IPv6 or DNS). The IP address of the interface configured as the SNTP client source interface.

Example: The following shows example CLI display output for the command.

```
(Routing) #show sntp source-interface
SNTP Client Source Interface.................. 0/2
SNTP Client Source IPv4 Address............... 192.168.2.20 [Up]
```

7.9. Time Zone Commands

7.9.1. clock set

This command sets the system time and date.

System time and date cannot be set when SNTP is enabled. If SNTP is enabled after you configure the system time and date, the SNTP clock takes precedence over the user-configured system time and date. If the platform supports real-time clock (RTC), the set time and date can be retained after a save and reload. Otherwise, the configured clock will not be retained across reloads.

Syntax	clock set hh:mm:ss / clock set mm/dd/yyyy
Command Mode	Global Config
<hh>	Hours in 24-hour format. The range is 0 to 23.
<mm>	Minutes, the range is 0 to 59.
<ss>	Seconds, the range is 0 to 59.
<mm>	Month, in 2-character numeric format. The range is 01 to 12.
<dd>	Day, in 2-character numeric format. The range is 01 to 31.
<yyyy>	Year, in 4-character numeric format. The range is 2010 to 2037.

Example: The following shows an example of the command.

```
(Routing)(Config)# clock set 03:17:00
(Routing) (Config)# clock set 11/01/2011
```

7.9.2. clock summer-time date

This command sets the Daylight Saving Time (DST), also known as summertime, offset to UTC. You have to specify the start year and end year along with the month, day, and time. If the optional parameters are not specified, they are read as either zero (0) or \0, as appropriate.

Syntax	clock summer-time date {date month year hh:mm date month year hh:mm}[offset offset] [zone acronym]
Command Mode	Global Config
<date>	Day of the month. The range is 1 to 31.
<month>	Month. The range is 1 to 12.
<year>	Year. The range is 2000 to 2097.
<offset>	The number of minutes to add during the summertime. The range is 1 to 1440.
<acronym>	The acronym for the time zone to be displayed when summertime is in effect. The range is up to four characters.

Example: The following shows examples of the command.

```
(Routing) (Config)# clock summer-time date 1 nov 2011 3:18 2 nov 2011 3:18
(Routing) (Config)# clock summer-time date 1 nov 2011 3:18 2 nov 2011 3:18
offset 120 zone INDA
```

7.9.3. clock summer-time recurring

This command sets the summertime offset to UTC recursively every year. This means that summertime will affect every year from the time of configuration. You have to specify the start and end parameters which include the month, day, and time. If the optional parameters are not specified, they are read as either zero (0) or \0, as appropriate.

Syntax	clock summer-time recurring {week day month hh:mm week day month hh:mm} [offset offset] [zone acronym]
Command Mode	Global Config
<week>	Week of the month. 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. hh range is 0 to 23, mm range is 0 to 59.
<offset>	The number of minutes to add during the summertime. The range is 1 to 1440.
<acronym>	The acronym for the time zone to be displayed when summertime is in effect. The range is up to four characters.

Example: The following shows examples of the command.

```
(Routing) (Config)# clock summer-time recurring 2 sun nov 3:18 2 mon nov
3:18
(Routing) (Config)# clock summer-time recurring 2 sun nov 3:18 2 mon
nov 3:18 offset 120 zone INDA
```

7.9.3.1. no clock summer-time

This command resets the summertime configuration.

Syntax	no clock summer-time
Command Mode	Global Config

Example: The following shows an example of the command.

```
(Routing) (Config)# no clock summer-time
```

7.9.4. clock timezone

This command sets the offset to Coordinated Universal Time (UTC). If the optional parameters are not specified, they will be read as either zero (0) or \0 as appropriate.

Syntax

Command Mode	Global Config
<hours>	Hours difference from UTC.
<minutes>	Minutes difference from UTC. The range is zero (0) to 59.
<acronym>	The acronym for the time zone. The range is up to four characters.

Example: The following shows an example of the command.

```
(Routing) (Config)# clock timezone 5 minutes 30 zone INDA
```

7.9.4.1. no clock timezone

This command resets the time zone settings.

Syntax	no clock timezone
Command Mode	Global Config

Example: The following shows an example of the command.

```
(Routing) (Config)# no clock timezone
```

7.9.5. show clock

This command displays the time and date from the system clock.

Syntax	show clock
Command Mode	Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(Routing) # show clock
15:02:09 (UTC+0:00) Nov 1 2011
No time source
```

Example: With the configuration above, the following output appears:

```
(Routing) # show clock
10:55:40 INDA(UTC+7:30) Nov 1 2011 No time source
```

7.9.6. show clock detail

This command displays the detailed system time along with the time zone and the summertime configuration.

Syntax	show clock detail
Command Mode	Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(Routing) # 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
```

Example: With the configuration above, the following output appears:

```
(Routing) # 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
```

7.10. DHCP Server Commands

This section describes the commands you to configure the DHCP server settings for the switch. DHCP uses UDP as its transport protocol and supports a number of features that facilitate in administration address allocations.

7.10.1. ip dhcp pool

This command configures a DHCP address pool name on a DHCP server and enters DHCP pool configuration mode.

Default	none
Syntax	ip dhcp pool name
Command Mode	Global Config

7.10.1.1. no ip dhcp pool

This command removes the DHCP address pool. The name should be previously configured pool name.

Syntax	no ip dhcp pool name
Command Mode	Global Config

7.10.2. client-identifier

This command specifies the unique identifier for a DHCP client. Unique-identifier is a valid notation in hexadecimal format. In some systems, such as Microsoft DHCP clients, the client identifier is required instead of hardware addresses. The unique-identifier is a concatenation of the media type and the MAC address. For example, the Microsoft client identifier for Ethernet address c819.2488.f177 is 01c8.1924.88f1.77 where 01 represents the Ethernet media type. For more information, refer to the „Address Resolution Protocol Parameters“ section of RFC 1700, Assigned Numbers for a list of media type codes.

Default	none
Syntax	client-identifier uniqueidentifier
Command Mode	DHCP Pool Config

7.10.2.1. no client-identifier

This command deletes the client identifier.

Syntax	no client-identifier
Command Mode	DHCP Pool Config

7.10.3. client-name

This command and specifies the name for a DHCP client. Name is a string consisting of standard ASCII characters.

Default	none
Syntax	client-name name
Command Mode	DHCP Pool Config

7.10.3.1. no client-name

This command removes the client name.

Syntax	no client-name
Command Mode	DHCP Pool Config

7.10.4. default-router

This command specifies the default router list for a DHCP client. *{address1, address2, … address8}* are valid IP addresses, each made up of four decimal bytes ranging from 0 to 255. IP address 0.0.0.0 is invalid.

Default	none
Syntax	default-router address1 [address2 … address8]
Command Mode	DHCP Pool Config

7.10.4.1. no default-router

This command removes the default router list.

Syntax	no default-router
Command Mode	DHCP Pool Config

7.10.5. dns-server

This command specifies the IP servers available to a DHCP client. Address parameters are valid IP address; each made up of four decimal bytes ranging from 0 to 255. IP address 0.0.0.0 is invalid.

Default	none
Syntax	dns-server address1 [address2 … address8]
Command Mode	DHCP Pool Config

7.10.6. hardware-address

This command specifies the hardware address of a DHCP client. Hardware-address is the MAC address of the hardware platform of the client consisting of 6 bytes in dotted hexadecimal format. Type indicates the protocol of the hardware platform. It is 1 for 10 MB Ethernet and 6 for IEEE 802.

Default	ethernet
Syntax	hardware-address hardwareaddress type
Command Mode	DHCP Pool Config

7.10.6.1. no hardware-address

This command removes the hardware address of the DHCP client.

Syntax	no hardware-address
Command Mode	DHCP Pool Config

7.10.7. host

This command specifies the IP address and network mask for a manual binding to a DHCP client. Address and Mask are valid IP addresses; each made up of four decimal bytes ranging from 0 to 255. IP address 0.0.0.0 is invalid. The prefix-length is an integer from 0 to 32.

Default	none
Syntax	Host address [{mask | prefix-length}]
Command Mode	DHCP Pool Config

7.10.7.1. no host

This command removes the IP address of the DHCP client.

Syntax	no host
Command Mode	DHCP Pool Config

7.10.8. lease

This command configures the duration of the lease for an IP address that is assigned from a DHCP server to a DHCP client. The overall lease time should be between 1-86400 minutes. If you specify *infinite*, the lease is set for 60 days. You can also specify a lease duration. *Days* is an integer from 0 to 59. *Hours* is an integer from 0 to 23. *Minutes* is an integer from 0 to 59.

Default	1 (day)

Syntax	lease [{days [hours] [minutes] | infinite}]
Command Mode	DHCP Pool Config

7.10.8.1. no lease

This command restores the default value of the lease time for DHCP server.

Syntax	no lease
Command Mode	DHCP Pool Config

7.10.9. network (DHCP Pool Config)

User this command to configure the subnet number and mask for a DHCP address pool on the server. Network-number is a valid IP address, made up of four decimal bytes ranging from 0 to 255. IP address 0.0.0.0 is invalid. Mask is the IP subnet mask for the specified address pool. The prefix-length is an integer from 0 to 32.

Default	none
Syntax	netwok networknumber [{mask | prefixLength}]
Command Mode	DHCP Pool Config

7.10.9.1. no network

This command removes the subnet number and mask.

Syntax	no network
Command Mode	DHCP Pool Config

7.10.10. bootfile

This command specifies the name of the default boot image for a DHCP client. The *filename* specifies the boot image file.

Syntax	bootfile filename
Command Mode	DHCP Pool Config

7.10.10.1. no bootfile

This command deletes the boot image name.

Syntax	no bootfile

Command Mode	DHCP Pool Config

7.10.11. domain-name

This command specifies the domain name for a DHCP client. The *domain* specifies the domain name string of the client.

Default	none
Syntax	domain-name domain
Command Mode	DHCP Pool Config

7.10.11.1. no domain-name

This command removes the domain name.

Syntax	no domain-name
Command Mode	DHCP Pool Config

7.10.12. netbios-name-server

This command configures NetBIOS Windows Internet Naming Service (WINS) name servers that are available to DHCP clients.

One IP address is required, although one can specify up to eight addresses in one command line. Servers are listed in order of preference (address1 is the most preferred server, address2 is the next most preferred server, and so on).

Default	none
Syntax	netbios-name-server address [address2 … address8]
Command Mode	DHCP Pool Config

7.10.12.1. no netbios-name-server

This command removes the NetBIOS name server list.

Syntax	no netbios-name-server
Command Mode	DHCP Pool Config

7.10.13. netbios-node-type

This command configures the NetBIOS node type for Microsoft Dynamic Host Configuration Protocol (DHCP) client type. Specifies the NetBIOS node type. Valid type are:

- b-node: Broadcast
- p-node: Peer-to-Peer
- m-node: Mixed
- h-node: Hybrid (recommended)

Default	none
Syntax	netbios-node-type type
Command Mode	DHCP Pool Config

7.10.13.1. no netbios-node-type

This command removes the NetBIOS node type.

Syntax	no netbios-node-type
Command Mode	DHCP Pool Config

7.10.14. next-server

This command cofigures the next server in the boot process of a DHCP client. The address parameter is the IP address of the next server in the boot process, which is typically a TFTP server.

Default	inbound interface helper addresses
Syntax	next-server address
Command Mode	DHCP Pool Config

7.10.14.1. no next-server

This command removes the boot server list.

Syntax	no next-server
Command Mode	DHCP Pool Config

7.10.15. option

This option command configures DHCP server options. The *code* parameter specifies the DHCP option code and ranges from 1-254. The *ascii string* parameter specifies an NVT ASCII character string. ASCII character strings that contain white space must be delimited by quotation marks. The *hex* string parameter specifies hexadecimal data. In hexadecimal, character strings are two hexadecimal digits. You can separate each byte by a period (for example, a3.4f.22.0c), colon (for example, a3:af:22:0c), or white space (for example, a3 4f 22 0c).

Default	none
Syntax	Option code {ascii string | hex string1 [string2 … string8] | ip address1 [address2 … address8]}
Command Mode	DHCP Pool Config

7.10.15.1. no option

This command removes the DHCP server options. The code parameter specifies the DHCP option code.

Syntax	no option code
Command Mode	DHCP Pool Config

7.10.16. ip dhcp excluded-address

This command specifies the IP addresses that a DHCP server should not assign to DHCP clients. Low-address and high-address are valid IP addresses; each made up of four decimal bytes ranging from 0 to 255. IP address 0.0.0.0 is invalid.

Default	none
Syntax	ip dhcp excluded-address lowaddress [highaddress]
Command Mode	Global Config

7.10.16.1. no ip dhcp excluded-address

This command removes the excluded IP addresses for a DHCP client. Low-address and high-address are valid IP addresses; each made up of four decimal bytes ranging from 0 to 255. IP address 0.0.0.0 is invalid.

Syntax	no ip dhcp excluded-address lowaddress [highaddress]
Command Mode	Global Config

7.10.17. ip dhcp ping packets

Use this command to specify the number, in a range from 2-10, of packets a DHCP server sends to a pool address as part of a ping operation. By default the number of packets sent to a pool address is 2, which is the smallest allowed number when sending packets. Setting the number of packets to 0 disables this command.

Default	2
Syntax	ip dhcp ping packets 0,2-10
Command Mode	Global Config

7.10.17.1. no ip dhcp ping packets

This command restores the number of ping packets to the default value.

Syntax	no ip dhcp ping packets
Command Mode	Global Config

7.10.18. service dhcp

This command enables the DHCP server.

Default	disable
Syntax	Service dhcp
Command Mode	Global Config

7.10.18.1. no service dhcp

This command disables the DHCP server.

Syntax	no service dhcp
Command Mode	Global Config

7.10.19. ip dhcp bootp automatic

This command enables the allocation of the addresses to the bootp client. The addresses are from the automatic address pool.

Default	disable
Syntax	ip dhcp bootp automatic
Command Mode	Global Config

7.10.19.1. no ip dhcp bootp automatic

This command disables the allocation of the addresses to the bootp client. The address are from the automatic address pool.

Syntax	no ip dhcp bootp automatic
Command Mode	Global Config

7.10.20. ip dhcp conflict logging

This command enables conflict logging on DHCP server.

Default	enabled
Syntax	ip dhcp conflict logging
Command Mode	Global Config

7.10.20.1. no ip dhcp conflict logging

This command disables conflict logging on DHCP server.

Syntax	no ip dhcp conflict logging
Command Mode	Global Config

7.10.21. clear ip dhcp binding

This command deletes an automatic address binding from the DHCP server database. If „*“ is specified, the bindings corresponding to all the addresses are deleted. *address* is a valid IP address made up of four decimal bytes ranging from 0 to 255. IP address 0.0.0.0 is invalid.

Syntax	clear ip dhcp binding {address | *}
Command Mode	Priviledged EXEC

7.10.22. clear ip dhcp server statistics

This command clears DHCP server statistics counters.

Syntax	clear ip dhcp server statistics
Command Mode	Priviledged EXEC

7.10.23. clear ip dhcp conflict

The command is used to clear an address conflict from the DHCP server database. The server detects conflicts using a ping. DHCP server clears all conflicts if the asterisk (*) character is used as the address parameter.

Default	none
Syntax	clear ip dhcp conflict {address | *}
Command Mode	Priviledged EXEC

7.10.24. show ip dhcp binding

This command displays address bindings for the specific IP address on the DHCP server. If no IP address is specified, the bindings corresponding to all the addresses are displayed.

Syntax show ip dhcp binding [address]

Command Mode Priviledged EXEC / User EXEC

Term	Definition
IP address	The IP address of the client.
Hardware Address	The MAC address or the client identifier.
Lease expiration	The lease expiration time of the IP address assigned to the client.
Type	The number in which IP address was assigned to the client.

7.10.25. show ip dhcp global configuration

This command displays address bindings for the specific IP address on the DHCP server. If no IP address is specified, the bindings corresponding to all the addresses are displayed.

Syntax show ip dhcp global configuration

Command Mode Priviledged EXEC / User EXEC

Term	Definition
Service DHCP	The field to display the status of dhcp protocol
Number of Ping Packets	The maximum number of Ping Packets that will be sent to verify that an IP address id not already assigned.
Conflict Logging	Shows whether conflict logging is enabled or disabled.
BootP Automatic	Shows whether BootP for dynamic pools is enabled or disabled.

7.10.26. show ip dhcp pool configuration

This command displays pool configuration. If all is specified, configuration for all the pools is displayed.

Syntax show ip dhcp poll configuration

Command Mode Priviledged EXEC / User EXEC

Term	Definition
Pool Name	The name of the configured pool.
Pool Type	The pool type.
Lease Time	The lease expiration time of the IP address assigned to the client.
DNS Servers	The list of DNS servers available to the DHCP client.
Default Routers	The list of the default routers available to the DHCP client.

The following additional field is displayed for Dynamic pool type:

Field	Definition
Network	The network number and the mask for the DHCP address pool.

The following additional fields are displayed for Manual pool type:

Field	Definition
Client Name	The name of a DHCP client.
Client Identifier	The unique identifier of a DHCP client.
Hardware Address	The hardware address of a DHCP client.
Hardware Address Type	The protocol of the hardware platform.
Host	The IP address and the mask for a manual binding to a DHCP client.

7.10.27. show ip dhcp server statistics

This command displays DHCP server statistics.

Syntax show ip dhcp server statistics

Command Mode Priviledged EXEC / User EXEC

Field	Definition
Automatic Bindings	The number of IP addresses that have been automatically mapped to the MAC addresses of hosts that are found in the DHCP database.
Expired Bindings	The number of expired leases.
Malformed Bindings	The number of truncated or corrupted messages that were received by the DHCP server.

Message Received:

Field	Definition
DHCP DISCOVER	The numer of DHCP DISCOVER messages the server has received.
DHCP REQUEST	The number of DHCP REQUEST messages the server has received.
DHCP DECLINE	The number of DHCP DECLINE messages the server has received.
DHCP RELEASE	The number of DHCP RELEASE messages the server has received.
DHCP INFORM	The number of DHCP INFORM messages the server has received.

Message Sent:

Field	Definition
DHCP OFFER	The number of DHCP OFFER messages the server sent.
DHCP ACK	The number of DHCP ACK messages the server sent.

Field	Definition
DHCP NACK	The number of DHCP NACK messages the server sent.

7.10.28. show ip dhcp conflict

This command displays address conflict logged by the DHCP server. If no IP address is specified, all the conflicting addresses are displayed.

Syntax show ip dhcp conflict [ip-address]

Command Mode Priviledged EXEC / User EXEC

Field	Definition
IP address	The IP address of the host as recorded on the DHCP server.
Detection Method	The manner in which the IP address of the hosts were found on the DHCP server.
Detection time	The time when the conflict was found.

7.11. 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.

7.11.1. ip domain lookup

Use this command to enable the DNS client.

Default	enabled
Syntax	ip domain lookup
Command Mode	Global Config

7.11.1.1. no ip domain lookup

Use this command to disable the DNS client.

Syntax	no ip domain lookup
Command Mode	Global Config

7.11.2. 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. The 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
Syntax	ip domain name name
Command Mode	Global Config

Example: 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.

7.11.2.1. no ip domain name

Use this command to remove the default domain name configured using the ip domain name command.

Syntax	no ip domain name
Command Mode	Global Config

7.11.3. 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 into this list.

Default	none
Syntax	ip domain list name
Command Mode	Global Config

7.11.3.1. no ip domain list

Use this command to delete a name from a list.

Syntax	no ip domain list name
Command Mode	Global Config

7.11.4. 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 address of the server. The preference of the servers is determined by the order they were entered.

Syntax	ip name-server server-address1 [server-address2…server-address8]
Command Mode	Global Config

7.11.4.1. no ip name server

Use this command to remove a name server.

Syntax	no ip name-server [server-address1…server-address8]
Command Mode	Global Config

7.11.5. ip name source-interface

Use this command to specify the physical or logical interface to use as the DNS client source interface. If configured, the address of source Interface is used for all DNS communications between the DNS server and the DNS client. Otherwise, there is no change in behavior. If the configured interface is down, the DNS client falls back to its default behavior.

Syntax	ip name source-interface {unit/slot/port | loopback loopback-id | tunnel tunnel-id | vlan vlan-id}

Command Mode	Global Config
<unit/slot/port>	Specifies the port to use as the source interface.
<loopback-id>	Specifies the loopback interface to use as the source interface. The range of the loopback ID is 0 to 7.
<tunnel-id>	Specifies the tunnel interface to use as the source interface. The range of the tunnel ID is 0 to 7.
<vlan-id>	Specifies the VLAN to use as the source interface.

7.11.5.1. no ip name source-interface

Use this command to reset the DNS source interface to the default settings.

Syntax	no ip name source-interface
Command Mode	Global Config

7.11.6. 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 one periods, hyphens, underscores, and non-consecutive spaces. Hostnames that include one or more space must be enclosed in quotation marks, for example, "lab-pc45".

Default	none
Syntax	ip host name ipaddress
Command Mode	Global Config

7.11.6.1. no ip host

Use this command to remove the name-to-address mapping.

Syntax	no ip host name
Command Mode	Global Config

7.11.7. 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
Syntax	ip domain retry number

Command Mode	Global Config

7.11.7.1. no ip domain retry

Use this command to return to the default.

Syntax	no ip domain retry number
Command Mode	Global Config

7.11.8. 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
Syntax	ip domain timeout seconds
Command Mode	Global Config

7.11.8.1. no ip domain timeout

Use this command to return to the default setting.

Syntax	no ip domain timeout seconds
Command Mode	Global Config

7.11.9. 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 IPv4 entries.

Syntax	clear host {name | all}
Command Mode	Privileged EXEC
<name>	A particular host entry to remove. The parameter name ranges from 1-255 characters.
<all>	Removes all entries.

7.11.10. 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 IPv4 entries.

Syntax show hosts [name]

Command Mode User EXEC

Parameter	Definition
Host Name	Domain host name.
Default Domain	Default domain name.
Default Domain List	Default domain list.
Domain Name Lookup	DNS client enabled/disabled.
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.

Example: The following shows example CLI display output for the command.

```
(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
Configured host name-to-address mapping:
Host                          Addresses
----------------------------- -----------------------------
accounting.gm.com             176.16.8.8
Host            Total    Elapsed Type    Addresses
--------------- -------- ------ -------- --------------
www.stanford.edu 72      3          IP       171.64.14.203
```

7.12. IP Address Conflict Commands

The commands in this section help troubleshoot IP address conflicts.

7.12.1. 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.

Syntax	ip address-conflict-detect run
Command Mode	Global Config

7.12.2. show ip address-conflict

This command displays the status information corresponding to the last detected address conflict.

Syntax	show ip address-conflict
Command Mode	Privileged EXEC

Parameter	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.

7.12.3. 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.

Syntax	clear ip address-conflict-detect [vrf vrf-name]
Command Mode	Privileged EXEC

7.13. Serviceability Packet Tracing Commands

These commands improve the capability of network engineers to diagnose conditions affecting their Fastpath product.

The output of **debug** commands can be long and may adversely affect system performance.

7.13.1. 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.

Syntax	capture start [{all | receive | transmit}]
Command Mode	Privileged EXEC
<all>	Capture all traffic.
<receive>	Capture only received traffic.
<transmit>	Capture only transmitted traffic.

7.13.2. capture stop

Use the command capture stop to manually stop capturing CPU packets for packet trace.

Syntax	capture stop
Command Mode	Privileged EXEC

7.13.3. capture file|remote|line

Use this command to configure file capture options. The command is persistent across a reboot cycle.

Syntax	capture {file|remote|line}

Command Mode Global Config

Parameter	Definition
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 automatically terminates any remote capture sessions and line capturing. After the packet capture is activated, the capture proceeds until the capture file reach its maximum size, or until the capture is stopped manually using the CLI command capture stop.
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, and 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 are a maximum 128 packets of maximum 128 bytes that can be captured and displayed in Line mode.

7.13.4. capture remote port

Use this command to configure file capture options. The command is persistent across a reboot cycle.

Syntax capture remote port id

Command Mode Global Config

7.13.5. capture file size

Use this command to configure file capture options. The command is persistent across a reboot cycle.

Syntax	capture file size max file size
Command Mode	Global Config

7.13.6. capture line wrap

This command enables wrapping of captured packets in line mode when the captured packets reaches full capacity.

Syntax	capture line wrap
Command Mode	Global Config

7.13.6.1. no capture line wrap

This command disables wrapping of captured packets and configures capture packet to stop when the captured packet capacity is full.

Syntax	no capture line wrap
Command Mode	Global Config

7.13.7. 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.

Syntax	show capture packets
Command Mode	Privileged EXEC

7.13.8. debug aaa accounting

This command is useful to debug accounting configuration and functionality in User Manager.

Syntax	debug aaa accounting
Command Mode	Privileged EXEC

7.13.8.1. no debug aaa accounting

Use this command to turn off debugging of User Manager accounting functionality.

Syntax	no debug aaa accounting
Command Mode	Privileged EXEC

7.13.9. debug arp

Use this command to enable ARP debug protocol messages. Optionally, a virtual router can be specified in which to execute the command.

Default	disabled
Syntax	debug arp [vrf vrf-name]
Command Mode	Privileged EXEC

7.13.9.1. no debug arp

Use this command to disable ARP debug protocol messages.

Syntax	no debug arp
Command Mode	Privileged EXEC

7.13.10. debug auto-voip

Use this command to enable Auto VOIP debug messages. Use the optional parameters to trace H323, SCCP, or SIP packets respectively.

Default	disabled
Syntax	debug auto-voip [H323|SCCP|SIP|oui]
Command Mode	Privileged EXEC

7.13.10.1. no debug auto-voip

Use this command to disable Auto VOIP debug messages.

Syntax	no debug auto-voip
Command Mode	Privileged EXEC

7.13.11. debug clear

This command disables all previously enabled

Default	disabled
Syntax	debug clear
Command Mode	Privileged EXEC

7.13.12. debug console

This command enables the display of 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
Syntax	debug console
Command Mode	Privileged EXEC

7.13.12.1. no debug console

This command disables the display of

Syntax	no debug console
Command Mode	Privileged EXEC

7.13.13. 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:

- Call stack information in both primitive and verbose forms
- 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
Syntax	debug crashlog {[kernel] crashlog-number [upload url] | proc | verbose | deleteall}
Command Mode	Privileged EXEC
<kernel>	View the crash log file for the kernel
<crashlog-number>	Specifies the file number to view. The system maintains up to four copies, and the valid range is 1-4.
<upload url>	To upload the crash log 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.

7.13.14. 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
Syntax	debug debug-config {download <url> | upload <url>}
Command Mode	Privileged EXEC

7.13.15. debug dhcp packet

This command displays from the local DHCPv4 client.

Default	disabled
Syntax	debug dhcp packet [transmit | receive]
Command Mode	Privileged EXEC

7.13.15.1. no debug dhcp

This command disables the display of

Syntax	no debug dhcp packet [transmit | receive]
Command Mode	Privileged EXEC

7.13.16. debug dot1x packet

Use this command to enable dot1x packet debug trace.

Default	disabled

Syntax	debug dot1x [transmit | receive]
Command Mode	Privileged EXEC

7.13.16.1. no debug dot1x packet

Use this command to disable dot1x packet debug trace.

Syntax	no debug dot1x [transmit | receive]
Command Mode	Privileged EXEC

7.13.17. debug igmpsnooping packet

This command enables tracing of IGMP Snooping packets received and transmitted by the switch.

Default	disabled
Syntax	debug igmpsnooping packet [transmit | receive]
Command Mode	Privileged EXEC

7.13.17.1. no debug igmpsnooping packet

This command disables tracing of IGMP Snooping packets.

Syntax	no debug igmpsnooping packet
Command Mode	Privileged EXEC

7.13.18. 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
Syntax	debug igmpsnooping packet transmit
Command Mode	Privileged EXEC

A sample output of the trace message is shown below:

```
  JAN 01 02:45:06 192.168.17.29-1
IGMPSNOOP[185429992]: igmp_snooping_debug.c(116)
908 % Pkt TX -
Intf: 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 on a non-stacking device.
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 Qurey – IGMP Membership Query • V1_Membership_Report – IGMP Version 1 Membership Report • V2_Membership_Report – IGMP Version 1 Membership Report • V3_Membership_Report – IGMP Version 1 Membership Report • V2_Leave_Group – IGMP Version 2 Leave Group
Group	Multicast group address in the IGMP header.

7.13.18.1. no debug igmpsnooping transmit

This command disables tracing of transmitted IGMP snooping packets.

Syntax	no debug igmpsnooping transmit
Command Mode	Privileged EXEC

7.13.19. 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
Syntax	debug igmpsnooping packet receive
Command Mode	Privileged EXEC

A sample output of the trace message is shown below:

```
  JAN 01 02:45:06 192.168.17.29-1
IGMPSNOOP[185429992]: igmp_snooping_debug.c(116)
908 % Pkt RX -
Intf: 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 on a non-stacking device.
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 Qurey – IGMP Membership Query • V1_Membership_Report – IGMP Version 1 Membership Report • V2_Membership_Report – IGMP Version 1 Membership Report • V3_Membership_Report – IGMP Version 1 Membership Report • V2_Leave_Group – IGMP Version 2 Leave Group
Group	Multicast group address in the IGMP header.

7.13.19.1. no debug igmpsnooping receive

This command disables tracing of received IGMP Snooping packets.

Syntax	no debug igmpsnooping receive
Command Mode	Privileged EXEC

7.13.20. debug ip acl

Use this command to enable debug of IP Protocol packets matching the ACL criteria.

Default	disabled
Syntax	debug ip acl acl Number
Command Mode	Privileged EXEC

7.13.20.1. no debug ip acl

Use this command to disable debug of IP Protocol packets matching the ACL criteria.

Syntax	no debug ip acl acl Number
Command Mode	Privileged EXEC

7.13.21. debug ipv6 dhcp

This command displays from the local DHCPv6 client.

Default	disabled
Syntax	debug ipv6 dhcp
Command Mode	Privileged EXEC

7.13.21.1. no debug ipv6 dhcp

This command disables the display of

Syntax	no debug ipv6 dhcp
Command Mode	Privileged EXEC

7.13.22. debug lacp packet

This command enables tracing of LACP packets received and transmitted by the switch.

Default	disabled
Syntax	debug lacp packet
Command Mode	Privileged EXEC

A sample output of the trace message is shown below:

```
  JAN 01 14:04:51 10.254.24.31-1
DOT3AD[183697744]: dot3ad_debug.c(385)
58 %% Pkt TX -
Intf: unit/slot/port(1), Type: LACP, Sys: 00:11:88:14:62:e1,
State: 0x47, Key: 0x36
```

7.13.22.1. no debug lacp packet

This command disables tracing of LACP packets.

Syntax	no debug lacp packet
Command Mode	Privileged EXEC

7.13.23. 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
Syntax	debug mldsnooping packet [receive | transmit]
Command Mode	Privileged EXEC

7.13.23.1. no debug mldsnooping packet

Use this command to disable debug tracing of MLD snooping packet reception and transmission.

Syntax	no debug mldsnooping packet [receive | transmit]
Command Mode	Privileged EXEC

7.13.24. 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
Syntax	debug ping packet [vrf vrf-name]
Command Mode	Privileged EXEC

A sample output of the trace message is shown below:

```
  JAN 01 00:21:22 192.168.17.29-1 SIM[181040176]: sim_debug.c(128)
20 % Pkt TX - Intf: 0/1(1), SRC_IP:10.50.50.2, DEST_IP:10.50.50.1,
Type:ECHO_REQUEST
  JAN 01 00:21:22 192.168.17.29-1 SIM[182813968]: sim_debug.c(82)
21 % Pkt RX - Intf: 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 for interfaces on a non-stacking device.
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.

7.13.24.1. no debug ping packet

This command disables tracing of ICMP echo requests and responses.

Syntax no debug ping packet

Command Mode Privileged EXEC

7.13.25. debug spanning-tree bpdu

This command enables tracing of spanning tree BPDUs received and transmitted by the switch.

Default disabled

Syntax debug spanning-tree bpdu

Command Mode Privileged EXEC

7.13.25.1. no debug spanning-tree bpdu

This command disables tracing of spanning tree BPDUs.

Syntax no debug spanning-tree bpdu

Command Mode Privileged EXEC

7.13.26. 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

Syntax debug spanning-tree bpdu receive

Command Mode Privileged EXEC

A sample output of the trace message is shown below:

```
  JAN 01 01:02:04 192.168.17.29-1 DOT1S[191096896]: dot1s_debug.c(1249)
101 % Pkt RX - Intf: 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 messages:

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.
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.

7.13.26.1. no debug spanning-tree bpdu receive

This command disables tracing of received spanning tree BPDUs.

Syntax no debug spanning-tree bpdu receive

Command Mode Privileged EXEC

7.13.27. 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

Syntax debug spanning-tree bpdu transmit

Command Mode Privileged EXEC

A sample output of the trace message is shown below:

```
  JAN 01 01:02:04 192.168.17.29-1 DOT1S[191096896]: dot1s_debug.c(1249)
101 % Pkt TX - Intf: 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.

7.13.27.1. no debug spanning-tree bpdu transmit

This command disables tracing of transmitted spanning tree BPDUs.

Syntax no debug spanning-tree bpdu transmit

Command Mode Privileged EXEC

7.13.28. debug tacacs

Use the debug tacacs packet command to turn on TACACS+ debugging.

Syntax debug tacacs {packet [receive | transmit] | accounting | authentication}

Command Mode Global Config

Parameter	Definition
packet receive	Turn on TACACS+ receive packet debugs.
packet transmit	Turn on TACACS+ transmit packet debugs.
accounting	Turn on TACACS+ authentication debugging.
authentication	Turn on TACACS+ authorization debugging.

7.13.29. debug transfer

This command enables debugging for file transfers.

Syntax debug transfer

Command Mode Privileged EXEC

7.13.29.1. no debug transfer

This command disables debugging for file transfers.

Syntax	no debug transfer
Command Mode	Privileged EXEC

7.13.30. show debugging

Use the show debugging command to display enabled packet tracing configurations.

Syntax	show debugging
Command Mode	Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(Routing)# debug arp
Arp packet tracing enabled.
(Routing)# show debugging
Arp packet tracing enabled.
```

7.13.31. mbuf

Use this command to configure memory buffer (MBUF) threshold limits and generate notifications when MBUF limits have been reached.

Syntax	mbuf {falling-threshold | rising threshold | severity}
Command Mode	Global Config

Field	Definition
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).

7.13.32. 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 the protocol is configured as *nfs*, this command mounts and unmounts the file system and informs the user of the status.

write core reloads the switch which is useful when the device malfunctions, but has not crashed.

For the **write core test** command, 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.

This command is only available on selected Linux-based platforms.

Default	None
Syntax	write core [test [dest_file_name]]
Command Mode	Privileged EXEC

7.13.33. show mbuf total

Use this command to display the memory buffer (MBUF) Utilization Monitoring parameters.

Syntax	show mbuf total
Command Mode	Privileged EXEC

Field	Definition
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.

7.14. 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 execute directly any of the BCM commands on the shell using the **bcmsh** command.

7.14.1. Bcmsh

The bcmsh command is used to enter into the BCM shell 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.

Syntax	bcmsh
Command Mode	Privileged EXEC

To exit the shell and return to the CLI, enter *exit*.

7.15. Cable Test Command

The cable test feature enables you to determine the cable connection status on a selected port.

The cable test feature is supported only for copper cable. It is not supported for optical fiber cable.

If the port has an active link while the cable test is run, the link can go down for the duration of the test.

7.15.1. cablestatus

This command returns the status of the specified port.

Syntax	cablestatus unit/slot/port
Command Mode	Privileged EXEC

Parameter	Definition
Cable Status	One of the following statuses is returned: • Normal: The cable is working correctly. • Open: The cable is disconnected or there is a faulty connector. • Short: There is an electrical short in the cable. • Cable Test Failed: The cable status could not be determined. The cable may in fact be working. • Crosstalk: There is crosstalk present on the cable. • No Cable: There is no cable present.
Cable Length	If this feature is supported by the PHY for the current link speed, the cable length is displayed as a range between the shortest estimated length and the longest estimated length. Note that if the link is down and a cable is attached to a 10/100 Ethernet adapter, then the cable status may display as Open or Short because some Ethernet adapters leave unused wire pairs unterminated or grounded. Unknown is displayed if the cable length could not be determined.

7.16. Switch Database Management Template Commands

A Switch Database Management (SDM) template is a description of the maximum resources a switch or router can use for various features. Different SDM templates allow different combinations of scaling factors, enabling different allocations of resources depending on how the device is used. In other words, SDM templates enable you to reallocate system resources to support a different mix of features based on your network requirements.

7.16.1. sdm prefer

Use this command to change the template that will be active after the next reboot. The keywords are as follows:

ipv4-routing - filters subsequent template choices to those that support IPv4, and not IPv6. The IPv4 routing *default* template maximizes the number of IPv4 unicast routes, while limiting the number of ECMP next hops in each route to 1.

After setting the template, you must reboot in order for the configuration change to take effect.

Default	ipv4-routing default
Syntax	sdm prefer {ipv4-routing | default}
Command Mode	Global Config

7.16.1.1. no sdm prefer

Use this command to clear the template configuration.

Syntax	no sdm prefer
Command Mode	Global Config

7.16.2. show sdm prefer

Use this command to view the currently active SDM template and its scaling parameters, or to view the scaling parameters for an inactive template. When invoked with no optional keywords, this command lists the currently active template and the template that will become active on the next reboot if it is different from the currently active template. If the system boots with a non-default template, and you clear the template configuration, either using **no sdm prefer** or by deleting the startup configuration, **show sdm prefer** lists the default template as the next active template. Use the optional keywords to list the scaling parameters of a specific template.

Syntax	show sdm prefer [ipv4-routing | default]

Command Mode Privileged EXEC

Parameter	Description
ARP Entries	The maximum number of entries in the IPv4 Address Resolution Protocol (ARP) cache for routing interfaces.
IPv4 Unicast Routes	The maximum number of IPv4 unicast forwarding table entries.
IPv6 NDP Entries	The maximum number of IPv6 Neighbor Discovery Protocol (NDP) cache entries.
IPv6 Unicast Routes	The maximum number of IPv6 unicast forwarding table entries.
ECMP Next Hops	The maximum number of next hops that can be installed in the IPv4 and IPv6 unicast forwarding tables.

Example: This example shows the current SDM template. The user has not changed the next active SDM template.

```
(router)#show sdm prefer
ARP Entries..................................... 238
IPv4 Unicast Routes............................. 16
IPv6 NDP Entries................................ 0
IPv6 Unicast Routes............................. 0
ECMP Next Hops.................................. 1
```

7.17. SFP Transceiver Commands

These commands show details for the SFP transceivers. Transceivers that are compliant with the SFF-8472(SFP+) and SFF-8436(QSFP+) standards are supported.

7.17.1. show fiber-ports optical-transceiver

This command displays the diagnostic information of the SFP. The values are derived from the SFP(Diagnostics) table using the I2c interface.

Syntax	show fiber-ports optical-transceiver {all|unit/slot/port}
Command Mode	Privileged EXEC

Parameter	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.

Example: The following shows example CLI display output for the command.

```
(Routing) #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
(Routing) #show fiber-ports optical-transceiver 0/49
                              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
```

7.17.2. show fiber-ports optical-transceiver-info

This command displays the SFP vendor-related information. The values are derived from the SFP using the I2c interface.

Syntax	show fiber-ports optical-transceiver-info {all|unit/slot/port}

Command Mode Privileged EXEC

Parameter	Description
Vendor Name	The vendor name is the full name of the corporation, an abbreviation for the name of the corporation, the SCSI company code for the corporation, or the stock exchange symbol for the corporation. The name is 1 to 16 ASCII characters in length.
Link Length 50um	This value specifies the link length that is supported by the transceiver while operating in compliance with applicable standards using 50-micron multimode OM2 [500 MHz * 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.
Link Length 62.5um	This value specifies the 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 be determined from the transceiver technology.
Serial Number	The vendor serial number for the transceiver. The serial number is 1 to 16 ASCII characters in length. A value of all zeros in the field indicates that the vendor serial number is unspecified.
Part Number	The vendor part number or product name. A value of all zeros in the 16-byte field indicates that the vendor part number is unspecified.
Nominal Bit Rate	The nominal bit (signaling) rate, 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 zero indicates that the bit rate is not specified and must be determined from the transceiver technology. The actual information transfer rate depends on the encoding of the data, as defined by the encoding value.
Rev	The vendor revision is unspecified.

Example: The following shows example CLI display output for the command.

```
(Switching) #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  NETGEAR      8    3     A7N2018414      AXM761           10300  10
0/51  NETGEAR      8    3     A7N2018472      AXM761           10300  10
0/52 NETGEAR       8    3     A7N2018501      AXM761           10300  10
```

```
(Switching) #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  NETGEAR      8    3     A7N2018414      AXM761           10300  10
```

7.18. Remote Monitoring Commands

Remote Monitoring (RMON) is a method of collecting a variety of data about the network traffic. RMON supports 64-bit counters (RFC 3273) and High Capacity Alarm Table (RFC 3434).

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.

7.18.1. rmon alarm

This command sets the RMON alarm entry in the RMON alarm MIB group.

Syntax rmon alarm alarm numbervariablesample interval {absolute|delta}rising-threshold value [rising-event-index] falling-threshold value [falling-event-index] [startup {rising|falling|rising-falling}] [owner string]

Command 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.
Alarm Absolute Value	The value of the statistic during the last sampling period. This object is a read-only, 32-bit signed value. The default is 1.
Alarm Rising Threshold	The rising threshold for the sample statistics. The range is 2147483648 to 2147483647. Thedefault 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*.

Example: The following shows an example of the command.

```
(Routing) (Config)# rmon alarm 1 ifInErrors.2 30 absolute rising-threshold
100 1 falling-threshold 10 2 startup rising owner myOwner
```

7.18.1.1. no rmon alarm

This command deletes the RMON alarm entry.

Syntax	no rmon alarm alarm number
Command Mode	Global Config

Example: The following shows an example of the command.

```
(Routing) (Config)# no rmon alarm 1
```

7.18.2. rmon hcalarm

This command sets the RMON hcalarm entry in the High Capacity RMON alarm MIB group.

Syntax	rmon hcalarm alarm numbervariablesample 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]
Command Mode	Global Config

Parameter	Description
High Capacity Alarm Index	An arbitrary integer index value used to identify uniquely 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 *AbsoluteValue* 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*.
High Capacity Alarm Rising-Threshold Absolute Value Low	The lower 32 bits of the absolute value for the threshold for the sampled statistic. The range is 0 to 4294967295. The default is 1.

Parameter	Description
High Capacity Alarm Rising-Threshold Absolute Value High	The upper 32 bits of the absolute value for the 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*.
Capacity Alarm Falling-Threshold Absolute Value Low	The lower 32 bits of the absolute value for the threshold for the sampled statistic. The range is 0 to 4294967295. The default is 1.
Capacity Alarm Falling-Threshold Absolute Value High	The upper 32 bits of the absolute value for the 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	The index of the eventEntry that is used when a falling threshold is crossed. The Falling Event Index 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*.

Example: The following shows an example of the command.

```
(Routing) (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
```

7.18.2.1. no rmon hcalarm

This command deletes the rmon hcalarm entry.

Syntax	no rmon hcalarm alarm number
Command Mode	Global Config

Example: The following shows an example of the command.

```
(Routing) (Config)# no rmon hcalarm 1
```

7.18.3. rmon event

This command sets the RMON event entry in the RMON event MIB group.

Syntax	rmon event event number [description string|log|owner string|trap community]
Command Mode	Global Config
<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, and LogSNMP Trap, Log and SNMP TrapThe 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.

Example: The following shows an example of the command.

```
(Routing) (Config)# rmon event 1 log description test
```

7.18.3.1. no rmon event

This command deletes the rmon event entry.

Syntax	no rmon event event number
Command Mode	Global Config

Example: The following shows an example of the command.

```
(Routing) (Config)# no rmon event 1
```

7.18.4. rmon collection history

This command sets the history control parameters of the RMON historyControl MIB group.

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.

Syntax	rmon collection history index number [buckets number|interval interval in sec| owner string]

Command Mode	Interface Config
<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.

Example: The following shows an example of the command.

```
(Routing) (Interface 0/1)# rmon collection history 1 buckets 10 interval 30
owner myOwner
```

Example: The following shows an example of the command.

```
(Routing) (Interface 0/1-0/10)#rmon collection history 1 buckets 10
interval 30 owner myOwner
Error: 'rmon collection history' is not supported on range of interfaces.
```

7.18.4.1. no rmon collection history

This command will delete the history control group entry with the specified index number.

Syntax	no rmon collection history index number
Command Mode	Interface Config

Example: The following shows an example of the command.

```
(Routing) (Interface 0/1-0/10)# no rmon collection history 1
```

7.18.5. show rmon

This command displays the entries in the RMON alarm table.

Syntax show rmon {alarms | alarm alarm-index}

Command 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.
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.
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*.

Example: The following shows example CLI display output for the command.

```
(Routing) #show rmon alarms
Index   OID                      Owner
----------------------------------------------
1       alarmInterval.1          MibBrowser
2       alarmInterval.1          MibBrowser
```

Example: The following shows example CLI display output for the command.

```
(Routing) #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
```

7.18.6. show rmon collection history

This command displays the entries in the RMON history control table.

Syntax	show rmon collection history [interfaces unit/slot/port]
Command 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.

Example: The following shows example CLI display output for the command.

```
(Routing) #show rmon collection history
Index   Interface Interval Requested Granted  Owner Samples
---------------------------------------------------------------
1       0/1       30       10        10       myowner
2       0/1       1800     50        10       monitorHistoryControl
3       0/2       30       50        10       monitorHistoryControl
4       0/2       1800     50        10       monitorHistoryControl
5       0/3       30       50        10       monitorHistoryControl
6       0/3       1800     50        10       monitorHistoryControl
7       0/4       30       50        10       monitorHistoryControl
--More-- or (q)uit
```

Example: The following shows example CLI display output for the command.

```
(Routing) #show rmon collection history interfaces 0/1
Index   Interface Interval Requested Granted  Owner Samples
---------------------------------------------------------------
1               0/1       30       10        10       myowner
2       0/1       1800     50        10       monitorHistoryControl
```

7.18.7. show rmon events

This command displays the entries in the RMON event table.

Syntax	show rmon events
Command 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*.
EventType	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.

Example: The following shows example CLI display output for the command.

```
(Routing) # show rmon events
Index Description Type Community Owner Last time sent
------------------------------------------------------------
1     test        log  public    MIB   0 days 0 h:0 m:0 s
```

7.18.8. show rmon history

This command displays the specified entry in the RMON history table.

Syntax	show rmon history index {errors [period seconds]|other [period seconds]| throughput [period seconds]}
Command 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.

Parameter	Description
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.
Maximum Table Size	A 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	A total number of undersize packets. Packets are less than 64 octets long (excluding framing bits, including FCS octets).
Oversize Packets	A total number of oversize packets. Packets are longer than 1518 octets (excluding framing bits, including FCS octets).
Fragments	A 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	A 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	A total number of octets received on the interface.
Packets	A total number of packets received (including error packets) on the interface.
Broadcast	A total number of good Broadcast packets received on the interface.
Multicast	A total number of good Multicast packets received on the interface.
Util	Port utilization of the interface associated with the history index specified.
Dropped Collisions	A total number of dropped collisions.

Example: The following shows example CLI display output for the command.

```
(Routing) #show rmon history 1 errors
Sample set: 1 Owner: myowner Interface: 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
```

Example: The following shows example CLI display output for the command.

```
(Routing) #show rmon history 1 throughput
Sample set: 1 Owner: myowner
Interface: 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
(Routing) #show rmon history 1 other
Sample set: 1 Owner: myowner
Interface: 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
```

7.18.9. show rmon log

This command displays the entries in the RMON log table.

Syntax	show rmon log [event-index]
Command 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.

Parameter	Description
Description	A comment describing the event entry for which the log is generated.
Time	Time at which the event is generated.

7.18.10. show rmon statistics interfaces

This command displays the RMON statistics for the giveninterfaces.

Syntax show rmon statistics interfaces unit/slot/port

Command Mode Privileged Exec

Parameter	Description
Port	unit/slot/port
Dropped	A total number of dropped events on the interface.
Octets	A total number of octets received on the interface.
Packets	A total number of packets received (including error packets) on the interface.
Broadcast	A total number of good broadcast packets received on the interface.
Multicast	A total number of good multicast packets received on the interface.
CRC Align Errors	A total number of packets received have a length (excluding framing bits, including FCS octets) of between 64 and 1518 octets inclusive.
Collisions	A total number of collisions on the interface.
Undersize Pkts	A total number of undersize packets. Packets are less than 64 octets long (excluding framing bits, including FCS octets).
Oversize Pkts	A total number of oversize packets. Packets are longer than 1518 octets (excluding framing bits, including FCS octets).
Fragments	A 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	A 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 the length or had a bad Frame Check Sequence (FCS).
64 Octets	A total number of packets which are 64 octets in length (excluding framing bits, including FCS octets).
65-127 Octets	A total number of packets which are between 65 and 127 octets in length (excluding framing bits, including FCS octets).
128-255 Octets	A total number of packets which are between 128 and 255 octets in length (excluding framing bits, including FCS octets).
256-511 Octets	A total number of packets which are between 256 and 511 octets in length (excluding framing bits, including FCS octets).

Parameter	Description
512-1023 Octets	A total number of packets which are between 512 and 1023 octets in length (excluding framing bits, including FCS octets).
1024-1518 Octets	A total number of packets which are between 1024 and 1518 octets in length (excluding framing bits, including FCS octets).
HC Overflow Pkts	A total number of HC overflow packets.
HC Overflow Octets	A total number of HC overflow octets.
HC Overflow Pkts 64 Octets	A total number of HC overflow packets which are 64 octets in length
HC Overflow Pkts 65 - 127 Octets	A total number of HC overflow packets which are between 65 and 127 octets in length.
HC Overflow Pkts 128 - 255 Octets	A total number of HC overflow packets which are between 128 and 255 octets in length.
HC Overflow Pkts 256 - 511 Octets	A total number of HC overflow packets which are between 256 and 511 octets in length.
HC Overflow Pkts 512 - 1023 Octets	A total number of HC overflow packets which are between 512 and 1023 octets in length.
HC Overflow Pkts 1024 - 1518 Octets	A total number of HC overflow packets which are between 1024 and 1518 octets in length.

Example: The following shows example CLI display output for the command.

```
(Routing) # show rmon statistics interfaces 0/1
Port: 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
```

7.18.11. show rmon hcalarms

This command displays the entries in the RMON high-capacity alarm table.

Syntax show rmon {hcalarms|hcalarm alarm index}

Command Mode Privileged Exec

Parameter	Description
High Capacity Alarm Index	An arbitrary integer index value used to identify uniquely 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 *AbsoluteValue* or *DeltaValue*. 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*.
High Capacity Alarm Rising-Threshold Absolute Value Low	The lower 32 bits of the absolute value for the 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 the 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 the 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 the 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*.

Example: The following shows example CLI display output for the command.

```
(Routing) #show rmon hcalarms
Index       OID                 Owner
----------------------------------------------
1           alarmInterval.1     MibBrowser
2           alarmInterval.1     MibBrowser
(Routing) #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
```

7.19. Statistics Application Commands

The statistics application gives you the ability to query for statistics on port utilization, flow-based and packet reception on programmable time slots. The statistics application collects the statistics at a configurable time range. You can specify the port number(s) or a range of ports for statistics to be displayed. The configured time range applies to all ports. Detailed statistics are collected between a specified time range in date and time format. You can define the time range as having an absolute time entry and/or a periodic time. For example, you can specify the statistics to be collected and displayed between 9:00 12 NOV 2011 (START) and 21:00 12 NOV 2012 (END) or schedule it on every Mon, Wed, and Fri 9:00 (START) to 21:00 (END).

You can configure the device to display statistics on the console. The collected statistics are presented on the console at END time.

7.19.1. stats group (Global Config)

This command creates a new group with the specified id or name and configures the time range and the reporting mechanism for that group.

Syntax	stats group group {id | name} timerange time range name reporting list of reporting methods
Command Mode	Global Config

Parameter	Description
group ID, name	Name of the group of statistics or its identifier to apply on the interface. The range is: 1. received 2. received-errors 3. transmitted 4. transmitted-errors 5. received-transmitted 6. port-utilization 7. congestion The default is None.
time range name	Name of the time range for the group or the flow-based rule. The range is 1 to 31 alphanumeric characters. The default is None.
list of reporting methods	Report the statistics to the configured method. The range is: 1. none 2. console

Parameter	Description
	3. syslog 4. e-mail The default is None.

Example: The following shows examples of the command.

```
(Routing) (Config)# stats group received timerange test reporting console
email syslog
(Routing) (Config)# stats group received-errors timerange test reporting
email syslog
(Routing) (Config)# stats group received-transmitted timerange test
reporting none
```

7.19.1.1. no stats group

This command deletes the configured group.

Syntax	no stats group group {id | name}
Command Mode	Global Config

Example: The following shows examples of the command.

```
(Routing) (Config)# no stats group received
(Routing) (Config)# no stats group received-errors
(Routing) (Config)# no stats group received-transmitted
```

7.19.2. stats flow-based (Global Config)

This command configures flow based statistics rules for the given parameters over the specified time range. Only an IPv4 address is allowed as source and destination IP address.

Syntax	stats flow-based rule-id timerange time range name [{srcip ip-address} {dstip ip-address} {srcmac mac-address} {dstmac mac-address} {srctcpport portid} {dsttcpport portid} {srcudpport portid} {dstudpport portid}]
Command Mode	Global Config

Parameter	Description
rule ID	The flow-based rule ID. The range is 1 to 16. The default is None.
time range name	Name of the time range for the group or the flow-based rule. The range is 1 to 31 alphanumeric characters. The default is None.
srcip ip-address	Configure the source IP address of the rule.
dstip ip-address	Configure the destination IP address of the rule.
srcmac mac-address	Configure the source MAC address of the rule

Parameter	Description
dstmac mac-address	Configure the destination MAC address of the rule.
srctcpport portid	Configure the source TCP port for the rule.
dsttcpport portid	Configure the destination TCP port for the rule.
srcudpport portid	Configure the source UDP port for the rule.
dstudpport portid	Configure the destination UDP port for the rule.

Example: The following shows examples of the command.

```
(Routing) (Config)# stats flow-based 1 timerange test srcip 1.1.1.1
dstip 2.2.2.2 srcmac 1234 dstmac 1234 srctcpport 123 dsttcpport 123
srcudpport 123 dstudpport 123
(Routing) (Config)#stats flow-based 2 timerange test srcip 1.1.1.1
dstip 2.2.2.2 srctcpport 123 dsttcpport 123 srcudpport 123 dstudpport 123
```

7.19.2.1. no stats flow-based

This command deletes flow-based statistics.

Syntax	stats flow-based rule-id
Command Mode	Global Config

Example: The following shows examples of the command.

```
(Routing) (Config)# no stats flow-based 1
(Routing) (Config)# no stats flow-based 2
```

7.19.3. stats flow-based reporting

This command configures the reporting mechanism for all the flow-based rules configured on the system.

There is no per flow-based rule reporting mechanism. Setting the reporting method as *none* resets all the reporting methods.

Syntax	stats flow-based reporting list of reporting methods
Command Mode	Global Config

Example: The following shows examples of the command.

```
(Routing) (Config)# stats flow-based reporting console email syslog
(Routing) (Config)# stats flow-based reporting email syslog
(Routing) (Config)# stats flow-based reporting none
```

7.19.4. stats group (Interface Config)

This command applies the group specified on an interface orinterface-range.

Syntax	stats group {group-id | name}
Command Mode	Interface Config

Parameter	Description
group id, name	Specify the ID or name of the group. The ID and name associations are as follows: 1. received 2. received-errors 3. transmitted 4. transmitted-errors 5. received-transmitted 6. port-utilization 7. congestion The default is None.

Example: The following shows examples of the command.

```
(Routing) (Interface 0/1-0/10)# stats group 1
(Routing) (Interface 0/1-0/10)# stats group 2
```

7.19.4.1. no stats group

This command deletes the interface or interface-range from the group specified.

Syntax	no stats group {group-id | name}
Command Mode	Interface Config

Example: The following shows examples of the command.

```
(Routing) (Interface 0/1-0/10)# no stats group 1
(Routing) (Interface 0/1-0/10)# no stats group 2
```

7.19.5. stats flow-based (Interface Config)

This command applies the flow-based rule specified by the id on an interface or interface-range.

Syntax	stats flow-based rule-id
Command Mode	Interface Config
<rule-id>	The flow-based rule ID. The range is 1 to 16. The default is None.

Example: The following shows examples of the command.

```
(Routing) (Interface 0/1-0/10)# stats flow-based 1
(Routing) (Interface 0/1-0/10)# stats flow-based 2
```

7.19.5.1. no stats flow-based

This command deletes the interface or interface-range from the flow-based rule specified.

Syntax	no stats flow-based rule-id
Command Mode	Interface Config

7.19.6. show stats group

This command displays the configured timerange and the interface list for the group specified and shows collected statistics for the specified time-range name on the interface list after the time-range expiry.

Syntax	show stats group {group-id | name}
Command Mode	Privileged EXEC

Parameter	Description
group id, name	Specify the ID or name of the group. The ID and name associations are as follows: 1. received 2. received-errors 3. transmitted 4. transmitted-errors 5. received-transmitted 6. port-utilization 7. congestion The default is None.

Example: The following shows example CLI display output for the command.

```
(Routing) #show stats group received
Group: received
Time Range: test
Interface List
-----------------
0/2, 0/4, lag 1
```

```
Counter ID                Interface Counter Value
------------------------- --------- ------------
Rx Total                  0/2       951600
Rx Total                  0/4       304512
Rx Total lag 1 0
Rx 64 0/2 0
Rx 64 0/4 4758
Rx 64 lag 1 0
Rx 65to128 0/2 0
Rx 65to128 0/4 0
Rx 65to128 lag 1 0
Rx 128to255 0/2 4758
Rx 128to255 0/4 0
Rx 128to255 lag 1 0
Rx 256to511 0/2 0
```

Example: The following shows example CLI display output for the command.

```
(Routing) #show stats group port-utilization
Group: port-utilization
Time Range: test
Interface List
--------------
0/2, 0/4, lag 1
Interface Utilization (%)
-------- ---------------
0/2      0
```

7.19.7. show stats flow-based

This command displays the configured timerange, flow-based rule parameters and the interface list for the flow specified.

Syntax	show stats flow-based {rule-id | all}
Command Mode	Privileged EXEC

Parameter	Description
rule-id	The flow-based rule ID. The range is 1 to 16. The default is None.

Example: The following shows example CLI display output for the command.

```
(Routing) #show stats flow-based all
Flow based rule Id.............................. 1
Time Range...................................... test
Source IP....................................... 1.1.1.1
Source MAC...................................... 1234
Source TCP Port................................. 123
Source UDP Port................................. 123
Destination IP.................................. 2.2.2.2
Destination MAC................................. 1234
```

```
Destination TCP Port..................... 123
Destination UDP Port..................... 123
Interface List
--------------
0/1 - 0/2
Interface Hit Count
--------- ---------
0/1 100
0/2 0
Flow based rule Id....................... 2
Time Range............................... test
Source IP................................ 1.1.1.1
Source TCP Port.......................... 123
Source UDP Port.......................... 123
Destination IP........................... 2.2.2.2
Destination TCP Port..................... 123
Destination UDP Port..................... 123
Interface List
--------------
0/1 - 0/2
Interface Hit Count
--------- ---------
0/1 100
0/2 0
```

Example: The following shows example CLI display output for the command.

```
(Routing) #show stats flow-based 2
Flow based rule Id....................... 2
Time Range............................... test
Source IP................................ 1.1.1.1
Source TCP Port.......................... 123
Source UDP Port.......................... 123
Destination IP........................... 2.2.2.2
Destination TCP Port..................... 123
Destination UDP Port..................... 123
Interface List
--------------
0/1 - 0/2
Interface Hit Count
--------- ---------
0/1 100
0/2 0
```

7.20. Green Ethernet Commands

This section describes the commands you use to configure Green Ethernet modes on the system. The purpose of the Green Ethernet features is to save power. FASTPATH suports the following three Green Ethernet modes:

- Energy-detect mode
- Short-reach mode
- Energy-efficient Ethernet (EEE) mode

Support for each Green Ethernet mode is platform dependent. The features and commands described in this section might not be available on your switch.

7.20.1. green-mode energy-detect

Use this command to enable energy-detect mode on an interfce or on a range of interfaces. With this mode enabled, when the port link is down, the port automatically powers down for short period of time and then wakes up to check link pulses. In energy-detect mode, the port can perform auto-negotiation and consume less power when no link partner is present.

Default	disabled
Syntax	green-mode energy-detect
Command Mode	Interface Config

7.20.1.1. no green-mode energy-detect

Use this command to disable energy-detect mode on the interface(s).

Syntax	no green-mode energy-detect
Command Mode	Interface Config

7.20.2. green-mode eee

Use this command to enable EEE low-power idle mode on an interface or on a range of interfaces. The EEE mode enables both send and receive sides of the link to disable some functionality for power saving when lightly loaded. The transition to EEE low-power mode does not change the port link status. Frames in transit are not dropped or corrupted in transition to and from this mode.

Default	disabled
Syntax	green-mode eee
Command Mode	Interface Config

7.20.2.1. no green-mode eee

Use this command to disable EEE mode on the interface(s).

Syntax	no green-mode eee
Command Mode	Interface Config

7.20.3. green-mode eee tx-idle-time

Use this command to configure the EEE mode transmit idle time for an interface or range of interfaces. The idle time is in microseconds. The transmit idle time is the amount of time the port waits before moving to the MAC TX transitions to the LPI state.

Default	0
Syntax	green-mode eee tx-idle-time 0-4294977295
Command Mode	Interface Config

7.20.3.1. no green-mode eee tx-idle-time

Use this command to return the EEE idle time to the default value.

Syntax	no green-mode eee tx-idle-time
Command Mode	Interface Config

7.20.4. green-mode eee tx-wake-time

Use this command to configure the EEE mode transmit wake time for an interface or range of interfaces. The wake time is in microseconds. The transmit wake time is the amount of time the switch must wait to go back to the ACTIVE state from the LPI state when it receives a packet for transmission.

Default	0
Syntax	green-mode eee t-wake-time 0-65535
Command Mode	Interface Config

7.20.4.1. no green-mode eee tx-wake-time

Use this command to return the EEE wake time to the default value.

Syntax	no green-mode eee tx-wake-time
Command Mode	Interface Config

7.20.5. green-mode eee-lpi-history sampling-interval

Use this command to configure global EEE LPI history collection interval for the system. The value specified in this command is applied globally on all interfaces in the switch or stack of switches. The sampling interval unit is seconds.

Default	3600

Syntax	green-mode eee-lpi-history sampling-interval 30-36000
Command Mode	Global Config

7.20.5.1. no green-mode eee-lpi-history sampling-interval

Use this command to return the global EEE LPI history collection interval to the default value.

Syntax	no green-mode eee-lpi-history sampling-interval
Command Mode	Global Config

7.20.6. green-mode eee-lpi-history max-samples

Use this command to configure global EEE LPI history collection buffer size for the system. The value specified in this command is applied globally on all interfaces in the switch or stack of switches.

Default	168
Syntax	green-mode eee-lpi-history max-samples 1-168
Command Mode	Global Config

7.20.7. no green-mode eee-lpi-history max-samples

Use this command to return the global EEE LPI history collection buffer size to the default value.

Syntax	no green-mode eee-lpi-history max-samples
Command Mode	Global Config

7.20.8. show green-mode

Use this command to display the green-mode configuration and operational status on all ports or on the specified port.

Syntax	show green-mode [slot/port]
Command Mode	Privileged EXEC

If you do not specify a port, the command displays the information in the following table.

Term	Description
Global	
Cumulative Energy Saving per Stack	Estimated Cumulative energy saved per stack in (Watts*hours) due to all green modes enabled.
Current Power Consumption per Stack	Power Consumption by all ports in stack in mWatts.

Term	Description
Power Saving	Estimated Percentage Power saved on all ports in stack due to Green mode(s) enabled.
Unit	Unit Index of the stack member
Green Ethernet Features supported	List of Green Features supported on the given unit which could be one or more of the following: Energy-Detect (Energy Detect), Short-Reach (Short Reach), EEE (Energy Efficient Ethernet), LPI-History (EEE Low Power Idle History), LLDP-Cap-Exchg (EEE LLDP Capability Exchange), Pwr-Usg-Est (Power Usage Estimates).
Energy Detect	
Energy-detect Config	Energy-detect Admin mode is enabled or disabled.
Energy-detect Opr	Energy detect mode is currently active or inactive. The energy detect mode may be administratively enabled, but the operational status may be inactive.
Short Reach	
Short-Reach Config auto	Short reach auto Admin mode is enabled or disabled.
Short-Reach Config forced	Short reach forced Admin mode is enabled or disabled.
Short-Reach Opr	Short reach mode is currently active or inactive. The short-reach mode may be administratively enabled, but the operational status may be inactive.
EEE	
EEE Config	EEE Admin mode is enabled or disabled.

If you specify the port, the command displays the information in the following table.

Term	Description
Energy Detect	
Energy-detect admin mode	Energy-detect mode is enabled or disabled.
Energy-detect operational status	Energy detect mode is currently active or inactive. The energy-detect mode may be administratively enabled, but the operational status may be inactive. The possible reasons for the status are described below.
Reason for Energy-detect current operational status	The energy detect mode may be administratively enabled, but the operational status may be inactive for one of the following reasons: • Port is currently operating in the fiber mode • Link is up • Admin Mode Disabled If the energy-detect operational status is active, this field displays *No energy detected*.

Term	Description
Short Reach	
Short-Reach auto Admin mode	Short reach auto mode is enabled or disabled.
Short-Reach force Admin mode	Short reach forced mode is enabled or disabled.
Short reach operational status	Short reach mode is currently active or inactive. The short-reach mode may be administratively enabled, but the operational status may be inactive.
Reason for Short Reach current operational status	The short-reach mode may be administratively enabled, but the operational status may be inactive for one of the following reasons: • Long cable > 10m • Link Down • Fiber • Admin Mode Disabled • Not At GIG speed • Cable length Unknown If the short reach operational status is active, this field displays one of the following reasons: • Short cable < 10m • Forced
EEE	
EEE Admin Mode	EEE Admin mode is enabled or disabled.
Transmit Idle Time	It is the time for which condition to move to LPI state is satisfied, at the end of which MAC TX transitions to LPI state. The Range is (0 to 429496729). The Default value is 0.
Transmit Wake Time	It is the time for which MAC / switch has to wait to go back to ACTIVE state from LPI state when it receives packet for transmission. The Range is (0 to 65535). The Default value is 0.
Rx Low Power Idle Event Count	This field is incremented each time MAC RX enters LPI IDLE state. Shows the total number of Rx LPI Events since EEE counters are last cleared.
Rx Low Power Idle Duration (uSec)	This field indicates duration of Rx LPI state in 10 us increments. Shows the total duration of Rx LPI since the EEE counters are last cleared.
Tx Low Power Idle Event Count	This field is incremented each time MAC TX enters LP IDLE state. Shows the total number of Tx LPI Events since EEE counters are last cleared.

Term	Description
Rx Low Power Idle Duration (uSec)	This field indicates duration of Tx LPI state in 10 us increments. Shows the total duration of Tx LPI since the EEE counters are last cleared.
Tw_sys_tx (uSec)	Integer that indicates the value of Tw_sys that the local system can support. This value is updated by the EEE DLL Transmitter state diagram.
Tw_sys Echo (uSec)	Integer that indicates the remote system's Transmit Tw_sys that was used by the local system to compute the Tw_sys that it wants to request from the remote system.
Tw_sys_rx (uSec)	Integer that indicates the value of Tw_sys that the local system requests from the remote system. This value is updated by the EEE Receiver L2 state diagram.
Tw_sys_rx Echo (uSec)	Integer that indicates the remote systems Receive Tw_sys that was used by the local system to compute the Tw_sys that it can support.
Fallback Tw_sys (uSec)	Integer that indicates the value of fallback Tw_sys that the local system requests from the remote system.
Remote Tw_sys_tx (uSec)	Integer that indicates the value of Tw_sys that the remote system can support.
Remote Tw_sys Echo (uSec)	Integer that indicates the value Transmit Tw_sys echoed back by the remote system.
Remote Tw_sys_rx (uSec)	Integer that indicates the value of Tw_sys that the remote system requests from the local system.
Remote Tw_sys_rx Echo (uSec)	Integer that indicates the value of Receive Tw_sys echoed back by the remote system.
Remote Fallback Tw_sys (uSec)	Integer that indicates the value of fallback Tw_sys that the remote system is advertising.
Tx_dll_enabled	Initialization status of the EEE transmit Data Link Layer management function on the local system.
Tx_dll_ready	Data Link Layer ready: This variable indicates that the TX system initialization is complete and is ready to update/receive LLDPDU containing EEE TLV. This variable is updated by the local system software.
Rx_dll_enabled	Status of the EEE capability negotiation on the local system.
Rx_dll_ready	Data Link Layer ready: This variable indicates that the RX system initialization is complete and is ready to update/receive LLDPDU containing EEE TLV. This variable is updated by the local system software.
Cumulative Energy Saving	Estimated Cumulative energy saved on this port in (Watts × hours) due to all green modes enabled.
Time Since Counters Last Cleared	Time Since Counters Last Cleared (since the time of power up, or after the clear eee statistics command is executed).

7.20.9. clear green-mode statistics

Use this command to clear the following Green Ethernet mode statistics:

- EEE LPI event count and LPI duration
- EEE LPI history table entries
- Cumulative power-savings estimates

You can clear the statistics for a specified port or for all ports.

Syntax	clear green-mode statistics {slot/port | all}
Command Mode	Privileged EXEC

7.20.10. show green-mode eee-lpi-history

Use this command to display interface green-mode EEE LPI history.

Syntax	show green-mode eee-lpi-history interface slot/port
Command Mode	Privileged EXEC

Term	Description
Sampling Interval	Interval at which EEE LPI statistics is collected.
Total No. of Samples to Keep	Maximum number of samples to keep.
Percentage LPI time per stack	Percentage of Total time spent in LPI mode by all port in stack when compared to total time since reset.
Sample No.	Sample Index
Sample Time	Time since last reset
%time spent in LPI mode since last sample	Percentage of time spent in LPI mode on this port when compared to sampling interval.
%time spent in LPI mode since last reset	Percentage of total time spent in LPI mode on this port when compared to time since reset.

7.21. Power over Ethernet Commands

This section describes the commands you use to configure Power over Ethernet(PoE) modes on the system. The purpose of the PoE feature is for the LAN switching infrastructure to provide power over a copper Ethernet cable to an endpoint or powered device.

7.21.1. poe

Use this command to enable the ability of the port to deliver a power. The factory default is Enable.

Default	enabled
Syntax	poe
Command Mode	Interface Config

7.21.1.1. no poe

Use this command to disable the ability of the port to deliver a power.

Syntax	no poe
Command Mode	Interface Config

7.21.2. show poe

Use this command to display status information about the PoE System feature on the device.

Syntax	show poe
Command Mode	Privileged EXEC

Term	Description
Firmware Version	Version of the PoE controller's FW image.
Power Status	Indicates the power status.
Available Power	Maximum amount of available power the system can deliver to all ports in milliWatts.
Consumed Power	Total amount of a power which is currently being delivered to all ports in milliWatts.
Power Management Mode	Describes or controls the power management algorithm used by the PSE to deliver power to the requesting PDs. • Static - It means power allocated for each port depends on the type of power threshold configured on the port. • Dynamic - It means that power consumption of each port is measured and calculated in real-time.

7.21.3. show poe port configuration

Use this command to display per-port PoE System settings.

Syntax show poe port configuration { all | slot/port}

Command Mode Privileged EXEC

Term	Description
Interface	Indicates the physical interface supported PoE system.
Admin Mode	Indicates the ability of the port to deliver a power.

7.21.4. show poe port info

Use this command to display interface status about the PoE System feature on the device.

Syntax show poe port info { all | slot/port}

Command Mode Privileged EXEC

Term	Description
Interface	Indicates the physical interface supported PoE system.
Port Status	Indicates the port status.
Class Info	The class information of the Powered Device (PD) defines the range of power a PD is drawing from the system.
Output Voltage (V)	Current voltage being delivered to device in Volts.
Output Current (mA)	Current being delivered to device in mA.
Output Power (mW)	Current power being delivered to device in milliWatts.
Temperature	The temperature measured at this port of the PoE Controller. It is measured in degree celsius.

Chapter 8. Switching Commands

This section describes the following switching commands available in the FASTPATH CLI:

Section 8.27, “LLDP-MED Commands”

Section 8.28, “Denial of Service Commands”

Section 8.29, “MAC Database Commands”

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.

8.1. Port Configuration Commands

This section describes the commands you use to view and configure port settings.

8.1.1. 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 unit/slot/port and ending unit/slot/port, separated by a hyphen.

Syntax	interface {unit/slot/port | unit/slot/port(startrange)-unit/slot/port(endrange)}
Command Mode	Global Config

Example: The following example enters Interface Config mode for port 0/1:

```
(Routing) #configure
(Routing) (config)#interface 1/0/1
(Routing) (interface 1/0/1)#
```

Example: The following example enters Interface Config mode for ports 0/1 through 0/4:

```
(Routing)#configure
(Routing) (config)#interface 1/0/1-1/0/4
(Routing) (interface 1/0/1-1/0/4)#
```

8.1.2. auto-negotiate

This command enables automatic negotiation on a port or range of ports.

Default	enabled
Syntax	auto-negotiate
Command Mode	Interface Config

8.1.2.1. no auto-negotiate

This command disables automatic negotiation on a port.

Automatic sensing is disabled when automatic negotiation is disabled.

Syntax	no auto-negotiate
Command Mode	Interface Config

8.1.3. auto-negotiate all

This command enables automatic negotiation on all ports.

Default	enabled
Syntax	auto-negotiate all
Command Mode	Global Config

8.1.3.1. no auto-negotiate all

This command disables automatic negotiation on all ports.

Syntax	no auto-negotiate all
Command Mode	Global Config

8.1.4. description

Use this command to create a description of an interface or range of interfaces.

Syntax	description *description*
Command Mode	Interface Config

8.1.5. media-type

Use this command to change between fiber and copper mode on the Combo port. Fiber port uses the fiber optics as a medium for communication (for example, example SFP ports).

Default	Auto-select, SFP preferred
Syntax	media-type {auto-select | rj45 | sfp }
Command Mode	Interface Config

8.1.5.1. no media-type

Use this command to revert the media-type configuration and configure the default value on the interface.

Syntax	no media-type
Command Mode	Interface Config

8.1.6. 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 1522-12288 for tagged packets and a valid integer between 1518 - 12288 for untagged packets.

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)
Syntax	mtu 1518-12288
Command Mode	Interface Config

8.1.6.1. no mtu

This command sets the default MTU size (in bytes) for the interface.

Syntax	no mtu
Command Mode	Interface Config

8.1.7. shutdown

This command disables a port or range of ports.

You can use the shutdown command on physical and port-channel (LAG) interfaces, but not on VLAN routing interfaces.

Default	enabled
Syntax	shutdown
Command Mode	Interface Config

8.1.7.1. no shutdown

This command enables a port.

Syntax	no shutdown
Command Mode	Interface Config

8.1.8. shutdown all

This command disables all ports.

You can use the **shutdown all** command on physical and port-channel (LAG) interfaces, but not on VLAN routing interfaces.

Default	enabled
Syntax	shutdown all
Command Mode	Global Config

8.1.8.1. no shutdown all

This command enables all ports.

Syntax	no shutdown all
Command Mode	Global Config

8.1.9. 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 halves 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.

For 10G and 1000M speed, the half-duplex is not supported.

For 10G Base-T port, 10G and 1G speed are only operated when auto-negotiation of the port is enabled.

Default	Auto-negotiation is enabled.
Syntax	speed auto { 10|100|1000|2.5G|10G|20G|25G|40G|50G|100G } [10|100|1000|2.5G|10G|20G|25G|40G|50G|100G] [half-duplex|full-duplex]
Syntax	speed { 10|100|1000|2.5G|10G|20G|25G|40G|50G|100G } { half-duplex|full-duplex }
Command Mode	Interface Config

8.1.10. show port

This command displays port information.

Syntax	show port {intf-range | all}
Command Mode	Privileged Exec

Parameter	Definition
Interface	unit/slot/port
Type	If not blank, this field indicates that this port is a special type of port. The possible values are: 1. **Mirror:** this port is a monitoring port 2. **PC Mbr:** this port is a member of a port-channel(LAG) 3. **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.

Example: The following command shows an example of the command output for all ports.

```
(Routing) #show port all
Admin Physical Physical Link Link   LACP   Actor
Intf      Type   Mode      Mode  Status Status Trap   Mode Timeout
--------- ------ --------- ---------- ---------- ------ ------- ------
1/0/1 Enable Auto 100 Full Up Enable Enable long
1/0/2 Enable Auto 100 Full Up Enable Enable long
1/0/3 Enable Auto Down Enable Enable long
1/0/4 Enable Auto 100 Full Up Enable Enable long
1/0/5 Enable Auto 100 Full Up Enable Enable long
1/0/6 Enable Auto 100 Full Up Enable Enable long
1/0/7 Enable Auto 100 Full Up Enable Enable long
1/0/8 Enable Auto 100 Full Up Enable Enable long
1/1/1 Enable Down Disable N/A N/A
1/1/2 Enable Down Disable N/A N/A
1/1/3 Enable Down Disable N/A N/A
1/1/4 Enable Down Disable N/A N/A
1/1/5 Enable Down Disable N/A N/A
1/1/6 Enable Down Disable N/A N/A
```

Example: The following command shows an example of the command output for a range of ports.

```
(Routing) #show port 1/0/1-1/1/6
Admin Physical Physical Link Link   LACP   Actor
```

```
Intf Type Mode  Mode Status Status Trap   Mode Timeout
--------- ------ --------- ---------- ---------- ------ ------- ------
1/0/1 Enable Auto 100 Full Up Enable Enable long
1/0/2 Enable Auto 100 Full Up Enable Enable long
1/0/3 Enable Auto Down Enable Enable long
1/0/4 Enable Auto 100 Full Up Enable Enable long
1/0/5 Enable Auto 100 Full Up Enable Enable long
1/0/6 Enable Auto 100 Full Up Enable Enable long
1/0/7 Enable Auto 100 Full Up Enable Enable long
1/0/8 Enable Auto 100 Full Up Enable Enable long
1/1/1 Enable Down Disable N/A N/A
1/1/2 Enable Down Disable N/A N/A
1/1/3 Enable Down Disable N/A N/A
1/1/4 Enable Down Disable N/A N/A
1/1/5 Enable Down Disable N/A N/A
1/1/6 Enable Down Disable N/A N/A
```

8.1.11. show port description

This command displays the interface description.

Syntax	show port description {unit/slot/port | lag lag-id}
Command Mode	Privileged Exec

Parameter	Definition
Interface	The unit/slot/port or LAG with the information to view.
ifIndex	The interface index number associated with the port.
Description	The description of the interface created by the command.
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.

Example: The following shows example CLI display output for the command.

```
(Switching) #show port description 1/0/1
Interface...........1/0/1
ifIndex.............1
Description.........
MAC address.........00:10:18:82:0C:10
Bit Offset Val......1
```

8.2. 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.

STP is enabled on the switch and on all ports and LAGs by default.

If STP is disabled, the system does not forward BPDU messages.

8.2.1. spanning-tree

This command sets the spanning-tree operational mode to enabled.

Default	enabled
Syntax	spanning-tree
Command Mode	Global Config

8.2.1.1. 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.

Syntax	no spanning-tree
Command Mode	Global Config

8.2.2. 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
Syntax	spanning-tree auto-edge
Command Mode	Interface Config

8.2.2.1. no spanning-tree auto-edge

This command resets the auto-edge status of the port to the default value.

Syntax	no spanning-tree auto-edge
Command Mode	Interface Config

8.2.3. 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 thespeed of the interface. To configure the cost manually, specify a cost value from 1 to 2 000.

Default	auto
Syntax	spanning-tree cost {cost | auto}
Command Mode	Interface Config

8.2.3.1. no spanning-tree cost

This command resets the auto-edge status of the port to the default value.

Syntax	no spanning-tree cost
Command Mode	Interface Config

8.2.4. spanning-tree bpdufilter

Use this command to enable BPDU Filter on an interface or range of interfaces.

If BPDU filtering is configured globally on the switch, the feature is automatically enabled on all operational ports where the Edge Port feature is enabled. These ports are typically connected to hosts that drop BPDUs. However, if an operational edge port receives a BPDU, the BPDU filtering feature doesn’t allow the port to participate in the spanning-tree calculation.

Enabling BPDU filtering on a specific port allows the port to drop any BPDUs it receives.

Default	disabled
Syntax	spanning-tree bpdufilter
Command Mode	Interface Config

8.2.4.1. no spanning-tree bpdufilter

Use this command to disable BPDU Filter on the interface or range of interfaces.

Default	disabled
Syntax	no spanning-tree bpdufilter
Command Mode	Interface Config

8.2.5. spanning-tree bpdufilter default

Use this command to enable BPDU Filter on all the edge port interfaces.

Default	disabled
Syntax	spanning-tree bpdufilter default
Command Mode	Global Config

8.2.5.1. no spanning-tree bpdufilter default

Use this command to disable BPDU Filter on all the edge port interfaces.

Default	disabled
Syntax	no spanning-tree bpdufilter default
Command Mode	Global Config

8.2.6. spanning-tree bpduflood

Use this command to enable BPDU Flood on an interface or range of interfaces.

The BPDU flooding feature determines the behavior of the switch when it receives a BPDU on a port that is disabled for spanning tree. If BPDU flooding is configured, the switch will flood the received BPDU to all same configured ports on the switch which are enabled BPDU flooding

Default	disabled
Syntax	spanning-tree bpduflood
Command Mode	Interface Config

8.2.6.1. no spanning-tree bpduflood

Use this command to disable BPDU Flood on the interface or range of interfaces.

Default	disabled
Syntax	no spanning-tree bpduflood
Command Mode	Interface Config

8.2.7. spanning-tree bpduguard

Use this command to enable BPDU Guard on the switch.

When the switch is used as an access layer device, most ports function as edge ports that connect to a device such as a desktop computer or file server. The port has a single, direct connection and is configured as an edge port to implement the fast transition to a forwarding state. When the port receives a BPDU packet, the system sets it to non-edge port and recalculates the spanning tree, which causes network topology flapping. In normal cases, these ports do not receive any BPDU packets. However, someone may forge BPDU to attack maliciously the switch and cause network flapping.

bpduguard can be enabled in RSTP to prevent such attacks. When bpduguard is enabled, the switch disables an edge port that has received BPDU and notifies the network manager about it.

Default	disabled
Syntax	spanning-tree bpduguard
Command Mode	Global Config

8.2.7.1. no spanning-tree bpduguard

Use this command to disable BPDU Guard on the switch.

Default	disabled
Syntax	no spanning-tree bpduguard
Command Mode	Global Config

8.2.8. spanning-tree bpdumigrationcheck

Use this command to force a transmission of rapid spanning tree (RSTP) and multiple spanning trees (MSTP) BPDUs. Use the unit/slot/port parameter to transmit a BPDU from a specified interface, or use the *all* keyword to transmit 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.

Syntax	spanning-tree bpdumigrationcheck {unit/slot/port | all}
Command Mode	Global Config

8.2.9. spanning-tree configuration name

This command sets the Configuration Identifier Name for use in identifying the configuration that thisswitch is currently using. The name is a string of up to 32 characters.

Default	The base MAC address displayed using hexadecimal notation as specified in IEEE 802 standard.
Syntax	spanning-tree configuration name name
Command Mode	Global Config

8.2.9.1. no spanning-tree configuration name

This command resets the Configuration Identifier Name to its default.

Syntax	no spanning-tree configuration name
Command Mode	Global Config

8.2.10. 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
Syntax	spanning-tree configuration revision 0-65535
Command Mode	Global Config

8.2.10.1. no spanning-tree configuration revision

This command sets the Configuration Identifier Revision Level for use in identifying the configurationthat this switch is currently using to the default value.

Syntax	no spanning-tree configuration revision
Command Mode	Global Config

8.2.11. spanning-tree edgeport

This command specifies that an interface (or range of interfaces) is an Edge Port within the commonand internal spanning tree. This allows this port to transition to Forwarding State without delay.

Syntax	spanning-tree edgeport
Command Mode	Interface Config

8.2.11.1. no spanning-tree edgeport

This command specifies that this port is not an Edge Port within the common and internal spanning tree.

Syntax	no spanning-tree edgeport
Command Mode	Interface Config

8.2.12. spanning-tree forceversion

This command sets the Force Protocol Version parameter to a new value.

Default	802.1s
Syntax	spanning-tree forceversion {802.1d | 802.1s | 802.1w}
Command 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).

8.2.12.1. no spanning-tree forceversion

This command sets the Force Protocol Version parameter to the default value.

Syntax	no spanning-tree forceversion
Command Mode	Global Config

8.2.13. 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.

Default	15
Syntax	spanning-tree forward-time 4-30
Command Mode	Global Config

8.2.13.1. no spanning-tree forward-time

This command sets the Bridge Forward Delay parameter for the common and internal spanning tree to the default value.

Syntax	no spanning-tree forward-time
Command Mode	Global Config

8.2.14. spanning-tree guard

This command selects whether loop guard or root guard is enabled on an interface or range ofinterfaces. If neither is enabled, then the port operates in accordance with the multiple spanning treep rotocol.

Default	none
Syntax	spanning-tree guard {none| root | loop}
Command Mode	Interface Config

8.2.14.1. no spanning-tree guard

This command disables loop guard or root guard on the interface.

Syntax	no spanning-tree guard
Command Mode	Interface Config

8.2.15. 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
Syntax	spanning-tree max-age 6-40
Command Mode	Global Config

8.2.15.1. no spanning-tree max-age

This command sets the Bridge Max Age parameter for the common and internal spanning tree to the default value.

Syntax	no spanning-tree max-age
Command Mode	Global Config

8.2.16. spanning-tree max-hops

This command sets the MSTP Max Hops parameter to a new value for the common and internal spanning tree. The max-hops value is a range from 1 to 127.

Default	20
Syntax	spanning-tree max-hops 1-127
Command Mode	Global Config

8.2.16.1. no spanning-tree max-hops

This command sets the Bridge Max Hops parameter for the common and internal spanning tree to the default value.

Syntax	no spanning-tree max-hops
Command Mode	Global Config

8.2.17. 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 anexisting 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 forthe 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
Syntax	spanning-tree mst mstid {{cost 1-200000000| auto} | port-priority 0-240}
Command Mode	Interface Config

8.2.17.1. 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.

Syntax	no spanning-tree mst mstid {cost | port-priority}
Command Mode	Interface Config

8.2.18. 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

Syntax	spanning-tree mst instance mstid
Command Mode	Global Config

8.2.18.1. 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.

Syntax	no spanning-tree mst instance mstid
Command Mode	Global Config

8.2.19. 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 61440 in increments of 4096.

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 61440. 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
Syntax	spanning-tree mst priority mstid 0-61440
Command Mode	Global Config

8.2.19.1. 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.

Syntax	no spanning-tree mst priority mstid
Command Mode	Global Config

8.2.20. spanning-tree mst vlan

This command adds an association between a multiple spanning tree instance and one or more VLANsso that the VLAN(s) are no longer associated with the common and internal spanning tree.

The parameter *mstid* is a number 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, each separated by a comma with no spaces in between. To specify arange of VLANs, separate the beginning and ending VLAN ID with a dash (-). The VLAN IDs may or may not exist in the system.

Syntax	spanning-tree mst vlan mstid vlanid
Command Mode	Global Config

8.2.20.1. 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.

Syntax	no spanning-tree mst vlan mstid vlanid
Command Mode	Global Config

8.2.21. spanning-tree port mode

This command sets the Administrative Switch Port State for this port to enabled.

Default	enabled
Syntax	spanning-tree port mode
Command Mode	Interface Config

8.2.21.1. no spanning-tree port mode

This command sets the Administrative Switch Port State for this port to disabled.

Syntax	no spanning-tree port mode
Command Mode	Interface Config

8.2.22. spanning-tree port mode all

This command sets the Administrative Switch Port State for all ports to enabled.

Default	enabled
Syntax	spanning-tree port mode all
Command Mode	Global Config

8.2.22.1. no spanning-tree port mode all

This command sets the Administrative Switch Port State for all ports to disabled.

Syntax	no spanning-tree port mode all
Command Mode	Global Config

8.2.23. spanning-tree transmit

This command sets the Bridge Transmit Hold Count parameter. The valid hold count range is 1-10.

Default	6
Syntax	spanning-tree transmit hold-count
Command Mode	Global Config
<hold-count>	The Bridge Tx hold-count parameter. The value in an integer between 1 and 10.

8.2.24. 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
Syntax	spanning-tree tcnguard
Command Mode	Interface Config

8.2.24.1. no spanning-tree tcnguard

This command resets the TCN guard status of the port to the default value.

Syntax	no spanning-tree tcnguard
Command Mode	Interface Config

8.2.25. spanning-tree vlan hello-time

Default	2 seconds
Syntax	spanning-tree vlan vlan-list hello-time 1-2
Command Mode	Global Config
<vlan-list>	The VLANs to which to apply this command.

<forward-time>	The spanning tree forward delay time. The range is 1-10 seconds.

8.2.26. show spanning-tree

This command displays spanning tree settings for the common and internal spanning tree. The following details are displayed.

Syntax	show spanning-tree
Command Mode	Privileged EXEC / User EXEC

Parameter	Description
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 of the bridge priority and the base MAC address of the bridge.
Root Path Cost	Value of the Root Path Cost parameter for the common and internal spanning tree.
Root Port Identifier	Identifier of the port to access the Designated Root for the CST
Root Port Max Age	Derived value.
Root Port Bridge Forward Delay	Derived value.
Hello Time	Configured value of the parameter for the CST.
Bridge Hold Time	Minimum time between transmission of Configuration Bridge Protocol Data Units (BPDUs).
Bridge Max Hops	Bridge max-hops count for the device.
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 FIDsList of forwarding database identifiers currently associated with this instance.
Associated FIDs	List of forwarding database identifiers currently associated with this instance.

Parameter	Description
Associated VLANs	List of VLAN IDs currently associated with this instance.

8.2.27. show spanning-tree brief

This command displays spanning tree settings for the bridge. The following information appears.

Syntax	show spanning-tree brief
Command Mode	Privileged EXEC / User EXEC

Parameter	Description
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).

8.2.28. show spanning-tree interface

This command displays the settings and parameters for a specific switch port within the common and internal spanning tree. The {unit/slot/port | lag lag-id} is the desired switch port or LAG to view. The following details are displayed on execution of the command.

Syntax	show spanning-tree interface {unit/slot/port | lag lag-id}
Command Mode	Privileged EXEC / User EXEC

Parameter	Description
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.

Parameter	Description
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 CountersLast Cleared	Time since port was reset, displayed in days, hours, minutes, and seconds.
STP BPDUs Transmitted	Spanning Tree Protocol Bridge Protocol Data Units sent.
STP BPDUs Received	Spanning Tree Protocol Bridge Protocol Data Units received.
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.

8.2.29. show spanning-tree mst detailed

This command displays the detailed settings for an MST instance.

Syntax	show spanning-tree mst detailed mstid
Command Mode	Privileged EXEC / User EXEC
<mstid>	A multiple spanning tree instance identifier. The value is 0

8.2.30. 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 {unit/slot/port | lag lag-id} is the desired switch port or LAG.

Syntax	show spanning-tree mst port detailed mstid {unit/slot/port | lag lag-id}
Command Mode	Privileged EXEC / User EXEC

Parameter	Description
MST Instance ID	The ID of the existing MST instance.
Port Identifier	The port identifier for the specified port within the selected MST instance. It is made up of 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.

Parameter	Description
Port Forwarding State	Current spanning tree state of this port.Port RoleEach 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 unit/slot/port is the desired switch port. In this case, the following are displayed.

Parameter	Description
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 PortPath 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.

Parameter	Description
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.
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.

8.2.31. show spanning-tree mst port summary

This command displays the settings of one or all ports within the specified multiple spanning treeinstance. The parameter mstid indicates a particular MST instance. The parameter {unit/slot/port| laglag-id | all} indicates the desired switch port, LAG, or all ports.

If you specify 0 (defined as the default CIST ID) as the mstid, the status summary displays for one or allports within the common and internal spanning tree.

Syntax	show spanning-tree mst port summary mstid {unit/slot/port | lag lag-id | all}
Command Mode	Privileged EXEC / User EXEC

Parameter	Description
MST Instance ID	The MST instance associated with this port.
Interface	unit/slot/port

Parameter	Description
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.

8.2.32. show spanning-tree mst port summary active

This command displays settings for the ports within the specified multiple spanning tree instance thatare active links.

Syntax show spanning-tree mst port summary mstid active

Command Mode Privileged EXEC / User EXEC

Parameter	Description
MST Instance ID	The MST instance associated with this port.
Interface	unit/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.

8.2.33. 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.

Syntax show spanning-tree mst summary

Command Mode Privileged EXEC / User EXEC

Parameter	Description
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.

8.2.34. 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.

Syntax	show spanning-tree summary
Command Mode	Privileged EXEC / User EXEC

Parameter	Description
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.

8.2.35. show spanning-tree vlan

This command displays the association between a VLAN and a multiple spanning tree instance. The vlanid corresponds to an existing VLAN ID.

Syntax	show spanning-tree vlan vlanid
Command Mode	Privileged EXEC / User EXEC

Parameter	Description
VLAN Identifier	The VLANs associated with the selected MST instance.
Associated Instance	Identifier for the associated multiple spanning tree instance or common and internal spanning tree.

8.3. VLAN Commands

This section describes the commands you use to configure VLAN settings.

8.3.1. vlan database

This command gives you access to the VLAN Config mode, which allows you to configure VLAN characteristics.

Syntax	vlan database
Command Mode	Privileged EXEC

8.3.2. network mgmt_vlan

This command configures the Management VLAN ID.

Default	1
Syntax	network mgmt_vlan 1-4093
Command Mode	Privileged EXEC

8.3.2.1. no network mgmt_vlan

This command sets the Management VLAN ID to the default.

Syntax	no network mgmt_vlan
Command Mode	Privileged EXEC

8.3.3. 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 1-4093.

After adding vlans from vlan 2 to vlan 4093, when you show it using command "show run", DUT console and ssh/telnet windows will be locked for some seconds.

Syntax	vlan 1-4093
Command Mode	VLAN Config

8.3.3.1. 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 1-4093.

When deleting vlans from vlan 2 to vlan 4093, DUT console and ssh/telnet windows are locked to avoid operation conflict.

Syntax	no vlan 1-4093
Command Mode	VLAN Config

8.3.4. 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. With either option, VLAN tagged frames are forwarded in accordance with the IEEE 802.1Q VLAN Specification.

Default	all
Syntax	vlan acceptframe {vlanonly | all}
Command Mode	Interface Config

8.3.4.1. no vlan acceptframe

This command resets the frame acceptance mode for the interface or range of interfaces to the default value.

Syntax	no vlan acceptframe
Command Mode	Interface Config

8.3.5. 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
Syntax	vlan ingressfilter
Command Mode	Interface Config

8.3.5.1. 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.

Syntax	no vlan ingressfilter
Command Mode	Interface Config

8.3.6. vlan internal allocation

Use this command to configure which VLAN IDs to use for port-based routing interfaces. When a port-based routing interface is created, an unused VLAN ID is assigned internally.

Syntax	vlan internal allocation {base vlan-id | policy ascending | policy decending}
Command Mode	Global Config
<base vlan-id>	The first VLAN ID to be assigned to a port-based routing interface.
<policy ascending>	VLAN IDs assigned to port-based routing interfaces start at the base and increase in value.
<policy descending>	VLAN IDs assigned to port-based routing interfaces start at the base and decrease in value.

8.3.7. vlan makestatic

This command changes a dynamically created VLAN to a static VLAN (one that is permanently configured and defined). The ID is a valid VLAN identification number. VLAN range is 1-4093.

Syntax	vlan makestatic 1-4093
Command Mode	VLAN Config

8.3.8. 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.

Syntax	vlan name 1-4093 name
Command Mode	VLAN Config

8.3.8.1. no vlan name

This command sets the name of a VLAN to a blank string.

Syntax	no vlan name 1-4093
Command Mode	VLAN Config

8.3.9. 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.

Syntax	vlan participation {exclude | include | auto} 1-4093
Command Mode	Interface Config
<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 and will not participate in this VLAN unless a join request is received on this interface. This is equivalent to registration normal.

8.3.10. vlan participation all

This command configures the degree of participation for all interfaces in a VLAN. The ID is a valid VLAN identification number.

Syntax	vlan participation all {exclude | include | auto} 1-4093
Command Mode	Global Config
<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 and will not participate in this VLAN unless a join request is received on this interface. This is equivalent to registration normal.

8.3.11. vlan port acceptframe all

This command sets the frame acceptance mode for all interfaces.

Default	all
Syntax	vlan port acceptframe all {vlanonly | all}
Command Mode	Global Config
<VLAN Only mode>	Untagged frames or priority frames received on this interface are discarded.
<Admit All mode>	Untagged frames or priority frames received on this interface are accepted and assignedthe 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.

8.3.11.1. 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.

Syntax	no vlan port acceptframe all
Command Mode	Global Config

8.3.12. 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
Syntax	vlan port ingressfilter all
Command Mode	Global Config

8.3.12.1. 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.

Syntax	no vlan port ingressfilter all
Command Mode	Global Config

8.3.13. vlan port pvid all

This command changes the VLAN ID for all interface.

Default	1
Syntax	vlan port pvid all 1-4093
Command Mode	Global Config

8.3.13.1. no vlan port pvid all

This command sets the VLAN ID for all interfaces to 1.

Syntax	no vlan port pvid all
Command Mode	Global Config

8.3.14. 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.

Syntax	vlan port tagging all 1-4093
Command Mode	Global Config

8.3.14.1. 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.

Syntax	no vlan port tagging all
Command Mode	Global Config

8.3.15. vlan pvid

This command changes the VLAN ID on an interface or range of interfaces.

Default	1
Syntax	vlan pvid 1-4093
Command Mode	Interface Config / Interface Range Config

8.3.15.1. no vlan pvid

This command sets the VLAN ID on an interface or range of interfaces to 1.

Syntax	no vlan pvid
Command Mode	Interface Config

8.3.16. 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.

Syntax	vlan tagging 1-4093
Command Mode	Interface Config

8.3.16.1. 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.

Syntax	no vlan tagging 1-4093
Command Mode	Interface Config

8.3.17. remote-span

This command identifies the VLAN as the RSPAN VLAN.

Default	None
Syntax	remote-span
Command Mode	VLAN configuration

8.3.18. 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.

Syntax	show vlan {vlanid|private-vlan [type]}
Command Mode	Privileged 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.

Term	Definition
Interface	The physical port, or LAG interface associated with the rest of the data in the row.
Current	The degree of participation of this port in this VLAN. The permissible values are: 1. Include - This port is always a member of this vlan. This is equivalent to registration fixed in the IEEE 802.1Q standard. 2. Exclude - This port is never a member of this VLAN. This is equivalent to registration forbidden in the IEEE 802.1Q standard. 3. 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: 1. Include - This port is always a member of this vlan. This is equivalent to registration fixed in the IEEE 802.1Q standard. 2. Exclude - This port is never a member of this VLAN. This is equivalent to registration forbidden in the IEEE 802.1Q standard. 3. 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.

8.3.19. show vlan internal usage

This command displays information about the VLAN ID allocation on the switch.

Syntax show vlan internal usage

Command Mode Privileged EXEC

Parameter	Definition
Base VLAN ID	Identifies the base VLAN ID for Internal allocation of VLANs to the routing interface.
Allocation policy	Identifies whether the system allocates VLAN IDs in ascending or descending order.

8.3.20. show vlan brief

This command displays a list of all configured VLANs.

Syntax show vlan brief

Command Mode Privileged EXEC

Parameter	Definition
VLAN ID	There is a VLAN Identifier (vlanid) associated with each VLAN. The range of the VLAN ID is 1-4093.
VLAN Name	A string associated with this VLAN as a convenience. It can be up to 32 alphanumericcharacters long, including blanks. The default is blank. VLAN ID 1 always has a name of The Deault.
VLAN Type	Type of VLAN, which can be Default (VLAN ID = 1) or static (one that is configured and permanently defined).

8.3.21. show vlan port

This command displays VLAN port information.

Syntax show vlan port {unit/slot/port | all}

Command Mode Privileged EXEC / User EXEC

Parameter	Definition
Interface	*unit/slot/port* It is possible to set the parameters for all ports by using the selectors on the top line.
Port VLAN ID	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.
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 by the 802.1Q VLAN specification.
Ingress Filtering	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 by the 802.1Q VLAN bridge specification. The factory default is disabled.
Default Priority	The 802.1p priority assigned to tagged packets arriving on the port.

8.4. 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.

8.4.1. switchport private-vlan

This command defines a private-VLAN association for an isolated or community port or a mapping for a promiscuous port.

Syntax	switchport private-vlan {host-association primary-vlan-id secondary-vlan-id | mapping primary-vlan-id {add | remove} secondary-vlan-list}
Command Mode	Interface Config
<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.

8.4.1.1. no switchport private-vlan

This command removes the private-VLAN association or mapping from the port.

Syntax	no switchport private-vlan {host-association|mapping}
Command Mode	Interface Config

8.4.2. 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
Syntax	switchport mode private-vlan {host|promiscuous}
Command Mode	Interface Config

<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.

8.4.2.1. no switchport mode private-vlan

This command removes the private-VLAN association or mapping from the port.

Syntax	no switchport mode private-vlan
Command Mode	Interface Config

8.4.3. private-vlan

This command configures the private VLANs and configures the association between the primary private VLAN and secondary VLANs.

Syntax	private-vlan {association [add|remove] secondary-vlan-list|community|isolated|primary}
Command Mode	VLAN Config
<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.

8.4.3.1. no private-vlan

This command restores normal VLAN configuration.

Syntax	
Command Mode	VLAN Config

8.5. 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 attach on voice components. QoS-based on IEEE 802.1P class of service (CoS) uses classification and scheduling to send 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.

8.5.1. voice vlan (Global Config)

Use this command to enable the Voice VLAN capability on the switch.

Default	disable
Syntax	Voice vlan
Command Mode	Global Config

8.5.1.1. no voice vlan (Global Config)

Use this command to disable the Voice VLAN capability on the switch.

Syntax	no voice vlan
Command Mode	Global Config

8.5.2. voice vlan (Interface Config)

Use this command to enable the Voice VLAN capability on the interface or range of interfaces.

Default	disable
Syntax	Voice vlan {vlanid id | dot1p priority | none | untagged}
Command 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.

Parameter	Description
none	Allow the IP phone to use its own configuration to send untagged voice traffic.
untagged	Configure the phone to send untagged voice traffic.

8.5.2.1. no voice vlan (Interface Config)

Use this command to disable the Voice VLAN capability on the interface.

Syntax	no voice vlan
Command Mode	Interface Config

8.5.3. 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
Syntax	voice vlan data priority {untrust | trust}
Command Mode	Interface Config

8.5.4. show voice vlan

Syntax	show voice vlan [interface {slot/port | all}]
Command Mode	Priviledged 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 dot1p 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.

Term	Definition
Voice VLAN Status	The operational status of Voice VLAN on the port.

8.6. 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 GVRP) or multicast groups (by using GMRP).

8.6.1. 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 intervel between the tansmission of GARP Protocol Data Unit (PDUs) registering (or re-registering) 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
Syntax	Set garp timer join 10-100
Command Mode	Interface Config / Global Config

8.6.1.1. no set garp timer join

This command sets the GVRP join time to the default and only has an effect when GVRP is enabled.

Syntax	no set garp timer join
Command Mode	Interface Config / Global Config

8.6.2. 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 registation 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 joine time.

Default	60
Syntax	Set garp timer leave 20-600
Command Mode	Interface Config / Global Config

8.6.2.1. 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.

Syntax	no set garp timer leave
Command Mode	Interface Config / Global Config

8.6.3. set garp timer leaveall

This command sets how frequently Leave All PDUs are generated. A Leave All PDU indicates that all registration 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
Syntax	set garp timer leaveall 200-6000
Command Mode	Interface Config / Global Config

8.6.3.1. 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.

Syntax	no set garp timer leaveall
Command Mode	Interface Config / Global Config

8.6.4. show garp

This command displays GARP information.

Syntax	show garp
Command 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.

8.7. 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 pruing.

If GVRP is disabled, the system does not forward GVRP messages.

8.7.1. set gvrp adminmode

This command enables GVRP on the system.

Default	disabled
Syntax	set gvrp adminmode
Command Mode	Privileged EXEC

8.7.1.1. no set gvrp adminmode

This command disables GVRP.

Syntax	no set gvrp adminmode
Command Mode	Privileged EXEC

8.7.2. 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
Syntax	set gvrp interfacemode
Command Mode	Interface Config / Interface Range / Global Config

8.7.2.1. 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.

Syntax	no set gvrp adminmode
Command Mode	Interface Config / Global Config

8.7.3. show gvrp configuration

This command displays Generic Attributes Registration Protocol (GVRP) information for one or all interfaces.

Syntax	show gvrp configuration {slot/port | all}
Command Mode	Privileged EXEC / User EXEC

Term	Definition
Interface	unit/slot/port.
Join Timer	The interval between the transmission of GARP PDUs registering (or re-registering) 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 value 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).
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 GVRP Mode	The GVRP 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.

8.8. 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.

If GMRP is disabled, the system does not forward GMRP messages.

8.8.1. set gmrp adminmode

This command enables GARP Multicast Registration Protocol (GMRP) on the system.

Default	disabled
Syntax	set gmrp interfacemode
Command Mode	Privileged EXEC

8.8.1.1. no set gmrp adminmode

This command disables GARP Multicast Registration Protocol (GMRP) on the system.

Syntax	no set gmrp interfacemode
Command Mode	Privileged EXEC

8.8.2. 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 enabled 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
Syntax	set gmrp interfacemode
Command Mode	Interface Config / Global Config

8.8.2.1. 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.

Syntax	no set gmrp interfacemode
Command Mode	Interface Config / Global Config

8.8.3. show gmrp configuration

This command displays Generic Attributes Registration Protocol (GARP) information for one or all interfaces.

Syntax	show gmrp configuration {slot/port | all}
Command Mode	Privileged EXEC / User EXEC

Term	Definition
Interface	unit/slot/port.
Join Timer	The interval between the transmission of GARP PDUs registering (or re-registering) 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 value 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).
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.

8.8.4. show mac-address-table gmrp

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

Syntax show mac-address-table gmrp

Command 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#.

8.9. Provisioning (IEEE 802.1p) Commands

This section describes the commands you use to configure provisioning (IEEE 802.1p,) which allows you to prioritize ports.

8.9.1. 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.

Syntax	vlan port priority all priority
Command Mode	Global Config

8.9.2. 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

Default	0
Syntax	vlan priority priority
Command Mode	Interface Config

8.10. 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.

8.10.1. 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.

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
Syntax	switchport protected groupid name name
Command Mode	Global Config

8.10.1.1. 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.

Syntax	no switchport protected groupid name
Command Mode	Global Config

8.10.2. 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.

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

Syntax	switchport protected groupid
Command Mode	Interface Config

8.10.2.1. 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.

Syntax	no switchport protected groupid
Command Mode	Interface Config

8.10.3. show switchport protected

This command displays the status of all the interfaces, including protected and unprotected interfaces.

Syntax	show switchport protected groupid
Command Mode	Privileged EXEC

Parameter	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.
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.

8.10.4. show interfaces switchport

This command displays the status of the interface (protected/unprotected) under the groupid.

Syntax	show interfaces switchport unit/slot/port groupid
Command Mode	Privileged EXEC

Parameter	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.

8.11. 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.

8.11.1. 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: conjunction with any one of the existing methods like local, radius, etc.

Syntax	aaa authentication dot1x default {[ias]|[method1 [method2 [method3]]]}
Command Mode	Global Config

Example: The following is an example of the command.

```
(Routing) #
(Routing) #configure
(Routing) (Config)#aaa authentication dot1x default ias none
(Routing) (Config)#aaa authentication dot1x default ias local radius none
```

8.11.2. clear dot1x statistics

This command resets the 802.1X statistics for the specified port or for all ports.

Syntax	clear dot1x statistics{unit/slot/port | all}
Command Mode	Privileged EXEC

8.11.3. clear dot1x authentication-history

This command clears the authentication history table captured during successful and unsuccessful authentication on all interface or the specified interface.

Syntax	clear dot1x authentication-history [unit/slot/port]
Command Mode	Privileged EXEC

8.11.4. clear radius statistics

This command is used to clear all RADIUSstatistics.

Syntax	clear radius statistics

Command Mode	Privileged EXEC

8.11.5. dot1x eapolflood

Use this command to enable EAPOL flood support on the switch.

Default	disabled
Syntax	dot1x eapolflood
Command Mode	Global Config

8.11.5.1. no dot1x eapolflood

This command disables EAPOL flooding on the switch.

Syntax	no dot1x eapolflood
Command Mode	Global Config

8.11.6. 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
Syntax	dot1x dynamic-vlan enable
Command Mode	Global Config

8.11.6.1. 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.

Syntax	no dot1x dynamic-vlan enable
Command Mode	Global Config

8.11.7. 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
Syntax	dot1x guest-vlan vlan-id

Command Mode	Interface Config

8.11.7.1. no dot1x guest-vlan

This command disables Guest VLAN on the interface.

Default	disabled
Syntax	no dot1x guest-vlan
Command Mode	Interface Config

8.11.8. 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.

Syntax	dot1x initialize unit/slot/port
Command Mode	Privileged EXEC

8.11.9. 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
Syntax	dot1x max-req count
Command Mode	Interface Config

8.11.9.1. 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.

Syntax	no dot1x max-req
Command Mode	Interface Config

8.11.10. 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	16
Syntax	dot1x max-users count
Command Mode	Interface Config

8.11.10.1. no dot1x max-users

This command resets the maximum number of clients allowed per port to its default value.

Syntax	no dot1x max-users
Command Mode	Interface Config

8.11.11. dot1x port-control

This command sets the authentication mode to use for 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
Syntax	dot1x port-control {force-unauthorized | force-authorized | auto | mac-based}
Command Mode	Interface Config

8.11.11.1. no dot1x port-control

This command sets the 802.1X port control mode on the specified port to the default value.

Syntax	no dot1x port-control
Command Mode	Interface Config

8.11.12. dot1x port-control all

This command sets the authentication mode to use for 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

Syntax	dot1x port-control all {force-unauthorized | force-authorized | auto | mac-based}
Command Mode	Global Config

8.11.12.1. no dot1x port-control all

This command sets the authentication mode on all ports to the default value.

Syntax	no dot1x port-control all
Command Mode	Global Config

8.11.13. dot1x re-authenticate

This command begins the re-authentication 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.

Syntax	dot1x re-authenticate unit/slot/port
Command Mode	Privileged EXEC

8.11.14. dot1x re-authentication

This command enables re-authentication of the supplicant for the specified interface or range of interfaces.

Default	disabled
Syntax	dot1x re-authentication
Command Mode	Interface Config

8.11.14.1. no dot1x re-authentication

This command disables re-authentication of the supplicant for the specified port.

Syntax	no dot1x re-authentication
Command Mode	Interface Config

8.11.15. 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
Syntax	dot1x system-auth-control

Command Mode	Global Config

8.11.15.1. no dot1x system-auth-control

This command is used to disable the dot1x authentication support on the switch.

Syntax	no dot1x system-auth-control
Command Mode	Global Config

8.11.16. 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
Syntax	dot1x system-auth-control monitor
Command Mode	Global Config

8.11.16.1. no dot1x system-auth-control monitor

This command disables the 802.1X Monitor mode on the switch.

Syntax	no dot1x system-auth-control monitor
Command Mode	Global Config

8.11.17. 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:

Token	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.
Reauthperiod	The value, in seconds, of the timer used by the authenticator state machine for this port to determine when reauthentication of the supplicant takes place. The reauth-period must be a value in the range 1 - 65535.

Token	Definition
quiet-period	The value, in seconds, of the timer used by the authenticator state machine for 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.
tx-period	The value, in seconds, of the timer used by the authenticator state machine for 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 for 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 for 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 / Resuth-period:3600 seconds / Quiet-period:60seconds / Tx-period:30 seconds / Supp-timeout:30 seconds / Server-timeout:30 seconds
Syntax	dot1x timeout {{guest-vlan-period seconds} |{reauth-period seconds} | {quiet-period seconds} | {tx-period seconds} | {supp-timeout seconds} | {server-timeout seconds}}
Command Mode	Interface Config

8.11.17.1. 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.

Syntax	no dot1x timeout {{guest-vlan-period seconds} |{reauth-period seconds} | {quiet-period seconds} | {tx-period seconds} | {supp-timeout seconds} | {server-timeout seconds}}
Command Mode	Interface Config

8.11.18. 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
Syntax	dot1x unauthenticated-vlan vlan id

Command Mode	Interface Config

8.11.18.1. no dot1x unauthenticated-vlan

This command resets the unauthenticated-vlan associated with the port to its default value.

Syntax	no dot1x unauthenticated-vlan
Command Mode	Interface Config

8.11.19. 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.

Syntax	dot1x user user {unit/slot/port | all}
Command Mode	Global Config

8.11.19.1. no dot1x user

This command removes the user from the list of users with access to the specified port or all ports.

Syntax	no dot1x user user {unit/slot/port | all}
Command Mode	Global Config

8.11.20. show authentication methods

This command displays the ordered authentication methods for all authentication login lists.

Syntax	show authentication methods
Command Mode	Privileged EXEC

Parameter	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.
Method 3	The third method in the specified authentication login list, if any.

Example: The following example displays the authentication configuration.

```
(Routing) #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       enableNetList
SSH     networkList       enableNetList
```

8.11.21. 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.

Syntax	show dot1x [{summary {unit/slot/port | all} | detail unit/slot/port | statistics unit/slot/port]
Command 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.

Parameter	Definition
Administrative Mode	Indicates whether authentication control on the switch is enabled or disabled.
VLAN Assignment Mode	Indicates whether the 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 {unit/slot/port | all}*, the dot1x configuration for the specified port or all ports are displayed.

Parameter	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.
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.

Parameter	Definition
Port Status	Indicates whether the port is authorized or unauthorized. Possible values are authorized / unauthorized.

Example: 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 *detailunit/slot/port*, the detailed dot1x configuration for the specified port is displayed.

Parameter	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.
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 for 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 for 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.
Supplicant Timeout	The timer used by the authenticator state machine for this port to timeout the supplicant. The value is expressed in seconds and will be in the range of 1 and 65535.

Parameter	Definition
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 for 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.
Vlan-assigned	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 for 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.
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.
Control Direction	The control direction for the specified port or ports. Possible values are both or in.
MaximumUsers	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 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 the 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.

Example: The following shows example CLI display output for the command.

```
(Routing) #show dot1x detail 0/1
Port..................................... 0/1
Protocol Version......................... 1
PAE Capabilities......................... Supplicant
Control Mode............................. auto
Supplicant PAE State..................... Initialize
Supplicant Backend Authentication State..... Initialize
Maximum Start trails..................... 3
Start Period (secs)...................... 30
```

```
Held Period (secs)............................ 60
Authentication Period (secs).................. 30
EAP Method.................................... MD5-Challenge
```

For each client authenticated on the port, the **show dot1x detail unit/slot/port** command will display the following MAC-based dot1x parameters if the port-control mode for that specific port is MAC-based.

Parameter	Definition
Supplicant MAC-Address	The MAC-address of the supplicant.
AuthenticatorPAE 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.
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 unit/slot/port*, the following dot1x statistics for the specified port appear.

Parameter	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.
EAP Request Frames Transmitted	The number of EAP request frames (other than request/identity frames) that have been transmitted by this authenticator.

Parameter	Definition
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.
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.

8.11.22. 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.

Syntax show dot1x authentication-history {unit/slot/port | all} [failed-auth-only] [detail]

Command Mode Privileged EXEC

Parameter	Definition
TimeStamp	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 Assigned, or Montior Mode VLAN ID.
Auth Status	The authentication status.
Reason	The actual reason behind the successful or failed authentication.

8.11.23. 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.

Syntax show dot1x clients {unit/slot/port | all} [detail]

Command Mode Privileged EXEC

Parameter	Definition
Clients Authenticated using Monitor Mode	Indicates the number of the Dot1x clients authenticated using Monitor mode.

Parameter	Definition
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.
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.

8.11.24. show dot1x users

This command displays 802.1X port security user information for locally configured users.

Syntax show dot1x usersunit/slot/port

Command Mode Privileged EXEC

Parameter	Definition
Users	Users configured locally to have access to the specified port.

8.12. 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.

8.12.1. dot1x pae

This command sets the port's dot1x role. The port can serve as either a supplicant or an authenticator.

Syntax	dot1x pae {supplicant | authenticator}
Command Mode	Interface Config

8.12.2. 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 to be moved from <authenticator to supplicant> or <supplicant to authenticator>, use this command.

Syntax	dot1x supplicant port-control {auto | force-authorized | force_unauthorized}
Command Mode	Interface Config
<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.

8.12.2.1. no dot1x supplicant port-control

This command sets the port-control mode to the default, auto.

Default	auto
Syntax	no dot1x supplicant port-control
Command Mode	Interface Config

8.12.3. 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
Syntax	dot1x supplicant max-start <1-10>
Command Mode	Interface Config

8.12.3.1. no dot1x supplicant max-start

This command sets the max-start value to the default.

Syntax	no dot1x supplicant max-start
Command Mode	Interface Config

8.12.4. 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
Syntax	dot1x supplicant timeout start-period <1-65535 seconds>
Command Mode	Interface Config

8.12.4.1. no dot1x supplicant timeout start-period

This command sets the start-period value to the default.

Syntax	no dot1x supplicant timeout start-period
Command Mode	Interface Config

8.12.5. dot1x supplicant timeout held-period

This command configures the held period timer interval to wait for the next authentication on previous authentication fail.

Default	30 seconds
Syntax	dot1x supplicant timeout held-period <1-65535 seconds>
Command Mode	Interface Config

8.12.5.1. no dot1x supplicant timeout held-period

This command sets the held-period value to the default value.

Syntax	no dot1x supplicant timeout held-period

Command Mode	Interface Config

8.12.6. 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
Syntax	dot1x supplicant timeout auth-period <1-65535 seconds>
Command Mode	Interface Config

8.12.6.1. no dot1x supplicant timeout auth-period

This command sets the auth-period value to the default value.

Syntax	no dot1x supplicant timeout auth-period
Command Mode	Interface Config

8.12.7. dot1x supplicant user

Use this command to map the given user to the port.

Syntax	dot1x supplicant user
Command Mode	Interface Config

8.12.8. show dot1x statistics

This command displays the dot1x port statistics in detail.

Syntax	show dot1x statistics unit/slot/port
Command Mode	Privileged EXEC / User EXEC

Parameter	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.

Parameter	Definition
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.

Example: The following shows example CLI display output for the command.

```
(Routing) #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
```

8.13. Flow Control Commands

This feature enables you to configure the switch to use symmetric, asymmetric or no flow control. Asymmetric flow control allows the switch to respond to received PAUSE frames, but the port cannot generate PAUSE frames. Symmetric flow control allows the switch to both responds to and generate MAC control PAUSE frames. This feature is typically used with iSCSI disk arrays.

802.3x Flow control, the MAC control PAUSE operation, is specified in IEEE 802.3 Annex 31 B. It allows traffic from one device to be throttled for a specified period of time and is defined for devices that are directly connected. A device that wishes to inhibit transmission of data frames from another device on the LAN transmits a PAUSE frame as defined in the IEEE specification.

When Symmetric flow control is enabled, the ports assert back pressure to the MAC, the MAC will respond by generating PAUSE frames, and the partner device will respond by stopping packet transmission to avoid packet loss. The ports are also capable of throttling the transmit rate in response to the PAUSE frames received from the peer. When transmission of symmetric flow control frames is enabled, the entire switch is placed in ingress drop mode. When in ingress drop mode, the switch will behave like any other ingress buffered switch and exhibit head of line blocking during times of congestion.

8.13.1. flowcontrol

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.

Support for asymmetric flow control is platform-dependent. For platforms that support only symmetric flow control, the {symmetric | asymmetric} keywords are not available.

Default	disabled
Syntax	flowcontrol
Command Mode	Privileged EXEC

8.13.1.1. no flowcontrol

Use this command to disable the symmetric flow control.

Syntax	no flowcontrol
Command Mode	Privileged EXEC

8.13.2. 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. It 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*.

Syntax show flowcontrol [unit/slot/port]

Command Mode Privileged EXEC

Parameter	Definition
Admin Flow Control	The administrative mode of flow control.
Port	The port associated with the rest of the data in the row.
Flow Control Oper	The operational mode of flow control.
RxPause	The received pause frame count.
TxPause	The transmitted pause frame count.

Example: The following shows example CLI display output for the command.

```
(Routing)#show flowcontrol
Admin Flow Control: Symmetric
Port Flow Control RxPause TxPause Oper
------ ------------ -------- ---------
0/1 Active 310 611
0/2 Inactive 0 0
--More-- or (q)uit
(Routing)#show flowcontrol interface 0/1
Admin Flow Control: Symmetric
Port Flow Control RxPause TxPause
                Oper
--------- ------- -------- -------
0/1 Active 310 611
```

8.14. 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 and unicast story recovery for individual interfaces. Unicast Storm-Control protects against traffic whose MAC addresses are not known by the system. For broadcast 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 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* form of storm-control maintains the configured level (to be active the next time that form of storm-control is enabled).

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.

8.14.1. 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	enabled
Syntax	storm-control broadcast
Command Mode	Global Config / Interface Config

8.14.1.1. no storm-control broadcast

Use this command to disable broadcast storm recovery mode for a specific interface or range of interfaces.

Syntax	no storm-control broadcast
Command Mode	Global Config / Interface Config

8.14.2. storm-control broadcast level

Use this command to configure the broadcast storm recovery threshold for an interface 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
Syntax	storm-control broadcast level 0-100
Command Mode	Global Config / Interface Config

8.14.2.1. no storm-control broadcast level

This command sets the broadcast storm recovery threshold to the default value for an interface and disables broadcast storm recovery.

Syntax	no storm-control broadcast level
Command Mode	Global Config / Interface Config

8.14.3. storm-control broadcast rate

Use this command to configure the broadcast storm recovery threshold for an interface 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
Syntax	storm-control broadcast rate 0-33554431
Command Mode	Global Config / Interface Config

8.14.3.1. no storm-control broadcast rate

This command sets the broadcast storm recovery threshold to the default value for an interface and disables broadcast storm recovery.

Syntax	no storm-control broadcast rate
Command Mode	Global Config / Interface Config

8.14.4. storm-control multicast

This command enables multicast storm recovery mode for an interface or range of interfaces. 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
Syntax	storm-control multicast
Command Mode	Global Config / Interface Config

8.14.4.1. no storm-control multicast

This command disables multicast storm recovery mode for an interface.

Syntax	no storm-control multicast
Command Mode	Global Config / Interface Config

8.14.5. storm-control multicast level

This command configures the multicast storm recovery threshold for an interface 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
Syntax	storm-control multicast level 0-100
Command Mode	Global Config / Interface Config

8.14.5.1. no storm-control multicast level

This command sets the multicast storm recovery threshold to the default value for an interface and disables multicast storm recovery.

Syntax	no storm-control multicast level 0-100
Command Mode	Global Config / Interface Config

8.14.6. storm-control multicast rate

Use this command to configure the multicast storm recovery threshold for an interface 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

Syntax	storm-control multicast rate 0-33554431
Command Mode	Global Config / Interface Config

8.14.6.1. no storm-control multicast rate

This command sets the multicast storm recovery threshold to the default value for an interface and disables multicast storm recovery.

Syntax	no storm-control multicast rate
Command Mode	Global Config / Interface Config

8.14.7. storm-control unicast

This command enables unicast storm recovery mode for an interface or range of interfaces. 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
Syntax	storm-control unicast
Command Mode	Global Config / Interface Config

8.14.7.1. no storm-control unicast

This command disables unicast storm recovery mode for an interface.

Syntax	no storm-control unicast
Command Mode	Global Config / Interface Config

8.14.8. storm-control unicast level

This command configures the unicast storm recovery threshold for an interface 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
Syntax	storm-control unicast level 0-100
Command Mode	Global Config / Interface Config

8.14.8.1. no storm-control unicast level

This command sets the unicast storm recovery threshold to the default value for an interface and disables unicast storm recovery.

Syntax	no storm-control unicast level
Command Mode	Global Config / Interface Config

8.14.9. storm-control unicast rate

Use this command to configure the unicast storm recovery threshold for an interface 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
Syntax	storm-control unicast rate 0-33554431
Command Mode	Global Config / Interface Config

8.14.9.1. no storm-control unicast rate

This command sets the unicast storm recovery threshold to the default value for an interface and disables unicast storm recovery.

Syntax	no storm-control unicast rate
Command Mode	Global Config / Interface Config

8.14.10. 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 *unit/slot/port* to display information about a specific interface.

Syntax	show storm-control [all | unit/slot/port]
Command Mode	Privileged EXEC

Parameter	Definition
Bcast Mode	Shows whether the broadcast storm control mode is enabled or disabled. The factory default is disabled.

Parameter	Definition
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.

Example: The following shows example CLI display output for the command.

```
(Routing) #show storm-control
Broadcast Storm Control Mode.................. Disable
Broadcast Storm Control Level................. 5 percent
Broadcast Storm Control Action................ None
Multicast Storm Control Mode.................. Disable
Multicast Storm Control Level................. 5 percent
Multicast Storm Control Action................ None
Unicast Storm Control Mode.................... Disable
Unicast Storm Control Level................... 5 percent
Unicast Storm Control Action.................. None
```

Example: The following shows example CLI display output for the command.

```
(Routing) #show storm-control 0/1
      Bcast   Bcast Bcast  Mcast   Mcast Mcast  Ucast   Ucast Ucast
Intf  Mode    Level Action Mode    Level Action Mode    Level Action
----- ------- ----- ------ ------- ----- ------ ------- ----- --------
1/0/1 Disable 5%    None   Disable 5%    None   Disable 5%    None
```

Example: The following shows an example of part of the CLI display output for the command.

```
(Routing) #show storm-control all
      Bcast   Bcast Bcast  Mcast   Mcast Mcast  Ucast   Ucast Ucast
Intf  Mode    Level Action Mode    Level Action Mode    Level Action
----- ------- ----- ------ ------- ----- ------ ------- ----- --------
1/0/1 Enable  5%    Trap   Disable 5%    None   Disable 5%    None
1/0/2 Enable  5%    Trap   Disable 5%    None   Disable 5%    None
1/0/3 Enable  5%    Trap   Disable 5%    None   Disable 5%    None
1/0/4 Enable  5%    Trap   Disable 5%    None   Disable 5%    None
1/0/5 Enable  5%    Trap   Disable 5%    None   Disable 5%    None
1/0/6 Enable  5%    Trap   Disable 5%    None   Disable 5%    None
```

8.15. 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.

8.15.1. 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.

Syntax	dhcp client vendor-id-option string
Command Mode	Global Config

8.15.1.1. 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.

Syntax	no dhcp client vendor-id-option
Command Mode	Global Config

8.15.2. 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.

Syntax	dhcp client vendor-id-option-string string
Command Mode	Global Config

8.15.2.1. no dhcp client vendor-id-option-string

This parameter clears the DHCP Vendor Option-60 string.

Syntax	no dhcp client vendor-id-option-string
Command Mode	Global Config

8.15.3. 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.

Syntax	show dhcp client vendor-id-option

Command Mode Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(Switching) #show dhcp client vendor-id-option
DHCP Client Vendor Identifier Option is Enabled
DHCP Client Vendor Identifier Option string is FASTPATHClient.
```

8.16. DHCP Snooping Configuration Commands

This section describes commands you use to configure DHCP Snooping.

8.16.1. ip dhcp snooping

Use this command to enable DHCP Snooping globally.

Default	disabled
Syntax	ip dhcp snooping
Command Mode	Global Config

8.16.1.1. no ip dhcp snooping

Use this command to disable DHCP Snooping globally.

Syntax	no ip dhcp snooping
Command Mode	Global Config

8.16.2. ip dhcp snooping vlan

Use this command to enable DHCP Snooping on a list of comma-separated VLAN ranges.

Default	disabled
Syntax	ip dhcp snooping vlan vlan-list
Command Mode	Global Config

8.16.2.1. no ip dhcp snooping vlan

Use this command to disable DHCP Snooping on VLANs.

Syntax	no ip dhcp snooping vlan vlan-list
Command Mode	Global Config

8.16.3. 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

Syntax	ip dhcp snooping verify mac-address
Command Mode	Global Config

8.16.3.1. no ip dhcp snooping verify mac-address

Use this command to disable verification of the source MAC address with the client hardware address.

Syntax	no ip dhcp snooping verify mac-address
Command Mode	Global Config

8.16.4. 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
Syntax	ip dhcp snooping database {local|tftp://hostIP/filename}
Command Mode	Global Config

8.16.5. 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
Syntax	ip dhcp snooping database write-delay in seconds
Command Mode	Global Config

8.16.5.1. no ip dhcp snooping database write-delay

Use this command to set the write delay value to the default value.

Syntax	no ip dhcp snooping database write-delay
Command Mode	Global Config

8.16.6. ip dhcp snooping binding

Use this command to configure static DHCP Snooping binding.

Syntax	ip dhcp snooping binding mac-address vlan vlanid ip address interface interfaceid

Command Mode	Global Config

8.16.6.1. no ip dhcp snooping binding

Use this command to remove the DHCP static entry from the DHCP Snooping database.

Syntax	no ip dhcp snooping binding mac-address
Command Mode	Global Config

8.16.7. 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 30 packets per second. The burst level range is 1 to 15 seconds.

Default	disabled (no limit)
Syntax	ip dhcp snooping limit {rate pps [burst interval seconds]}
Command Mode	Interface Config

8.16.7.1. 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.

Syntax	no ip dhcp snooping limit
Command Mode	Interface Config

8.16.8. 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
Syntax	ip dhcp snooping log-invalid
Command Mode	Interface Config

8.16.8.1. no ip dhcp snooping log-invalid

Use this command to disable the logging DHCP messages filtration by the DHCP Snooping application.

Syntax	no ip dhcp snooping log-invalid

Command Mode	Interface Config

8.16.9. ip dhcp snooping trust

Use this command to configure an interface or range of interfaces as trusted.

Default	disabled
Syntax	ip dhcp snooping trust
Command Mode	Interface Config

8.16.9.1. no ip dhcp snooping trust

Use this command to configure the port as untrusted.

Syntax	no ip dhcp snooping trust
Command Mode	Interface Config

8.16.10. show ip dhcp snooping

Use this command to display the DHCP Snooping global configurations and per port configurations.

Syntax	show ip dhcp snooping
Command 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.

Example: The following shows example CLI display output for the command.

```
(switch) #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
```

8.16.11. 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 DHCP 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.

Syntax	show ip dhcp snooping binding [{static/dynamic}] [interface unit/unit/slot/port] [vlan id]
Command 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.

Example: The following shows example CLI display output for the command.

```
(switch) #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
```

8.16.12. show ip dhcp snooping database

Use this command to display the DHCP Snooping configuration related to the database persistency.

Syntax	show ip dhcp snooping database
Command Mode	Privileged EXEC / User EXEC

Term	Definition
Agent URL	Bindings database agent URL.
Write Delay	The maximum write time to write the database into local or remote.

Example: The following shows example CLI display output for the command.

```
(switch) #show ip dhcp snooping database
agent url: /10.131.13.79:/sai1.txt
write-delay: 5000
```

8.16.13. show ip dhcp snooping interfaces

Use this command to show the DHCP Snooping status of the interfaces.

Syntax	show ip dhcp snooping interfaces
Command Mode	Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(Routing) #show ip dhcp snooping interfaces
Interface   Trust State Rate Limit  Burst Interval
                        (pps)        (seconds)
----------- ----------  ----------  --------------
1/g1        No          15          1
1/g2        No          15          1
1/g3        No          15          1
(Routing) #show ip dhcp snooping interfaces ethernet 0/15
Interface   Trust State Rate Limit  Burst Interval
                        (pps)        (seconds)
----------- ----------  ----------  --------------
1/g1        No          15          1
```

8.16.14. show ip dhcp snooping statistics

Use this command to list statistics for DHCP Snooping security violations on untrusted ports.

Syntax	show ip dhcp snooping statistics
Command Mode	Privileged EXEC / User EXEC

Term	Definition
Interface	The IP address of the interface in unit/unit/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 IfcMismatch	Represents the number of DHCP release and Deny messages received on the different portsthan learned previously.

Term	Definition
DHCP Server MAC Verify	Represents the number of DHCP server messages received on Untrusted ports.

Example: The following shows example CLI display output for the command.

```
(switch) #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
```

8.16.15. clear ip dhcp snooping binding

Use this command to clear all DHCP Snooping bindings on all interfaces or on a specific interface.

Syntax	clear ip dhcp snooping binding [interface unit/unit/slot/port]
Command Mode	Privileged EXEC / User EXEC

8.16.16. clear ip dhcp snooping statistics

Use this command to clear all DHCP Snooping statistics.

Syntax	clear ip dhcp snooping statistics
Command Mode	Privileged EXEC / User EXEC

8.17. 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 on 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.

If you configure the maximum number of dynamic port-channels (LAGs) that your platform supports, additional port-channels that you configure are automatically static.

8.17.1. port-channel

This command configures a new port-channel (LAG) and generates a logical unit/slot/port number for the port-channel. The name field is a character string which allows the dash characters. Use the **show port-channel** command to display the unit/slot/port number for the logical interface.

Before you include a port in a port-channel, set the port physical mode.

Syntax	port-channel name
Command Mode	Global Config

8.17.2. addport

This command adds one port to the port-channel (LAG). The first interface is a logical unit/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.

Before adding a port to a port-channel, set the physical mode of the port.

Syntax	addport logical unit/slot/port
Command Mode	Interface Config

8.17.3. deleteport (Interface Config)

This command deletes a port or a range of ports from the port-channel (LAG). The interface is a logical unit/slot/port number of a configured port-channel (or range of port-channels).

Syntax	deleteport logical unit/slot/port
Command Mode	Interface Config

8.17.4. deleteport (Global Config)

This command deletes all configured ports from the port-channel (LAG). The interface is a logicalunit/slot/port number of a configured port-channel .

Syntax	deleteport {logical unit/slot/port | all}
Command Mode	Global Config

8.17.5. lacp admin key

Use this command to configure the administrative value of the key for the port-channel. The value range of the key is 0 to 65535. This command can be used to configure a single interface or a range of interfaces.

Default	0x8000
Syntax	lacp admin key key
Command Mode	Interface Config

This command is applicable only to port-channel interfaces.

8.17.5.1. no lacp admin key

Use this command to configure the default administrative value of the key for the port-channel.

Syntax	no lacp admin key
Command Mode	Interface Config

8.17.6. 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	0

Syntax	lacp collector max delay delay
Command Mode	Interface Config

This command is applicable only to port-channel interfaces.

8.17.6.1. no lacp collector max delay

Use this command to configure the default port-channel collector max delay.

Syntax	no lacp collector max delay
Command Mode	Interface Config

8.17.7. 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
Syntax	lacp actor admin key key
Command Mode	Interface Config

This command is applicable only to physical interfaces.

8.17.7.1. no lacp actor admin key

Use this command to configure the default administrative value of the key.

Syntax	no lacp actor admin key
Command Mode	Interface Config

8.17.8. 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	0x05
Syntax	lacp actor admin state {individual|longtimeout|passive}
Command Mode	Interface Config

This command is applicable only to physical interfaces.

8.17.8.1. no lacp actor admin state

Use this command the configure the default administrative values of actor state as transmitted by the Actor in LACPDUs.

Syntax	no lacp actor admin state {individual|longtimeout|passive}
Command Mode	Interface Config

8.17.9. 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
Syntax	lacp actor port priority 0-65535
Command Mode	Interface Config

This command is applicable only to physical interfaces.

8.17.9.1. no lacp actor port priority

Use this command to configure the default priority value assigned to the Aggregation Port.

Syntax	no lacp actor port priority
Command Mode	Interface Config

8.17.10. interface lag

Use this command to enter Interface configuration mode for the specified LAG.

Syntax	interface lag lag-interface-number
Command Mode	Global Config

8.17.11. 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
Syntax	port-channel static
Command Mode	Interface Config

8.17.11.1. 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).

Syntax	no port-channel static
Command Mode	Interface Config

8.17.12. port lacpmode

This command enables Link Aggregation Control Protocol (LACP) on a port or range of ports.

Default	enabled
Syntax	port lacpmode
Command Mode	Interface Config

8.17.12.1. no port lacpmode

This command disables Link Aggregation Control Protocol (LACP) on a port.

Syntax	no port lacpmode
Command Mode	Interface Config

8.17.13. port lacpmode enable all

This command enables Link Aggregation Control Protocol (LACP) on all ports.

Syntax	port lacpmode enable all
Command Mode	Global Config

8.17.13.1. no port lacpmode enable all

This command disables Link Aggregation Control Protocol (LACP) on all ports.

Syntax	no port lacpmode enable all

Command Mode	Global Config

8.17.14. port lacptimeout (Interface Config)

This command sets the timeout on a physical interface or range of interfaces of a particular device type (actor) to either long or short timeout.

Default	long
Syntax	port lacptimeout {actor } {long | short}
Command Mode	Interface Config

8.17.14.1. no port lacptimeout

This command sets the timeout back to its default value on a physical interface of a particular device type (actor).

Syntax	no port lacptimeout { actor }
Command Mode	Interface Config

8.17.15. port lacptimeout (Global Config)

This command sets the timeout for all interfaces of a particular device type (actor) to either long or short timeout.

Default	long
Syntax	port lacptimeout { actor } {long | short}
Command Mode	Global Config

8.17.15.1. no port lacptimeout

This command sets the timeout for all physical interfaces of a particular device type (actor) back to their default values.

Syntax	no port lacptimeout { actor }
Command Mode	Global Config

8.17.16. port-channel adminmode

This command enables a port-channel (LAG). The option all sets every configured port-channel with the same administrative mode setting.

Syntax	port-channel adminmode [all]

Command Mode	Global Config

8.17.16.1. no port-channel adminmode

This command disables a port-channel (LAG). The option all sets every configured port-channel with the same administrative mode setting.

Syntax	no port-channel adminmode [all]
Command Mode	Global Config

8.17.17. port-channel linktrap

This command enables link trap notifications for the port-channel (LAG). The interface is a logicalunit/slot/port for a configured port-channel. The option all sets every configured port-channel with the same administrative mode setting.

Default	enabled
Syntax	port-channel linktrap {logical unit/slot/port | all}
Command Mode	Global Config

8.17.17.1. 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.

Syntax	no port-channel linktrap {logical unit/slot/port | all}
Command Mode	Global Config

8.17.18. 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.

Default	3
Syntax	port-channel load-balance {1 | 2 | 3 | 4 | 5 | 6 | 7}{unit/slot/port | all}
Command Mode	Global Config / Interface Config
<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
<unit/slot/port| all>	Global Config Mode only: The interface is a logical unit/slot/port number of a configured port-channel. All applies the command to all currently configured port-channels.

8.17.18.1. no port-channel load-balance

This command reverts to the default load balancing configuration.

Syntax	no port-channel load-balance {unit/slot/port | all}
Command Mode	Interface Config / Global Config
<unit/slot/port| all>	Global Config Mode only: The interface is a logical unit/slot/port number of a configured port-channel. All applies the command to all currently configured port-channels.

8.17.19. port-channel min-links

This command configures the port-channel

Default	1
Syntax	port-channel min-links 1-32
Command Mode	Interface Config

8.17.20. port-channel name

This command defines a name for the port-channel (LAG). The interface is a logical unit/slot/port for a configured port-channel, and name is a string up to 15 characters.

Syntax	port-channel name {logical unit/slot/port} name
Command Mode	Global Config

8.17.21. port-channel system priority

Use this command to configure port-channel system priority. The valid range of priority is 0-65535.

Default	0x8000
Syntax	port-channel system priority priority

Command Mode	Global Config

8.17.21.1. no port-channel system priority

Use this command to configure the default port-channel system priority value.

Syntax	no port-channel system priority
Command Mode	Global Config

8.17.22. show lacp actor

Use this command to display LACP actor attributes.

Syntax	show lacp actor {unit/slot/port|all}
Command Mode	Global Config

The following output parameters are displayed:

Parameter	Definition
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.

8.17.23. show lacp partner

Use this command to display LACP partner attributes.

Syntax	show lacp actor {unit/slot/port|all}
Command Mode	Privileged EXEC

The following output parameters are displayed:

Parameter	Definition
System Priority	The administrative value of priority associated with the Partner
System-ID	Represents the administrative value of the Aggregation Port
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.

8.17.24. 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.

Syntax	show port-channel brief
Command Mode	Privileged EXEC

For each port-channel the following information is displayed:

Parameter	Definition
Logical Interface	The unit/slot/port of the logical interface.
Port-channel Name	The name of the 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.

8.17.25. show port-channel

This command displays an overview of all port-channels (LAGs) on the switch. Instead of unit/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.

Syntax	show port-channel
Command Mode	Privileged EXEC

Term	Definition
Local Interface	The valid unit/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
Port-Channel Min-links	If the port-channel members are less than min-links, the link state will down.

Term	Definition
Admin Key	The administrative value of the Key for the protocol Partner.
Load Balance Option	The load balance option associated with this LAG.
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 unit/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).
Port Speed	Speed of the port-channel port.
Active Ports	This field lists ports that are actively participating in the port-channel (LAG).

Example: The following shows example CLI display output for the command.

```
(Switch) #show port-channel 3/1
Local Interface............................... 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      True
    partner/long
1/0/4 actor/long                Auto      True
    partner/long
```

8.17.26. show port-channel system priority

Use this command to display the port-channel system priority.

Syntax	show port-channel system priority
Command Mode	Privileged EXEC

8.17.27. show port-channel counters

Use this command to display port-channel counters for the specified port.

Syntax	show port-channel slot/port counters
Command 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.

Example: The following shows example CLI display output for the command.

```
(Espada) #show port-channel 0/3/1 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
```

8.17.28. clear port-channel counters

Use this command to clear and reset specified port-channel and member flap counters for the specified interface.

Syntax	clear port-channel {lag-intf-num | unit/slot/port} counters
Command Mode	Privileged EXEC

8.17.29. clear port-channel all counters

Use this command to clear and reset all port-channel and member flap counters for the specified interface.

Syntax	clear port-channel all counters
Command Mode	Privileged EXEC

8.18. Port Mirroring

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.

8.18.1. monitor session

This command configures a probe port and a monitored port for monitor session (port monitoring). Use the source interface *unit/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.

The source and destination cannot be configured as remote on the same device.

The reflector-port is configured at the source switch along with the destination RSPAN VLAN. The *reflector-port* forwards the mirrored traffic towards the destination switch.

This port must be configured with RSPAN VLAN membership.

Use the *destination interface unit/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.

Syntax	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 }
Command Mode	Global Config

Example: To configure the RSPAN VLAN source:

```
monitor session session-id source {interface unit/slot/port | vlan vlan-id |
remote vlan vlan-id }[rx/tx]
```

Example: To the configure RSPAN VLAN destination:

```
monitor session session-id destination {interface unit/slot/port |remote vlan
vlan-id reflector-port unit/slot/port}
```

8.18.1.1. 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 *unit/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

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.

Syntax	no monitor session session-id { interface unit/slot/port |remote vlan vlan-id reflector-port unit/slot/port }
Command Mode	Global Config

8.18.2. 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. In the current version of the software, the session-id parameter is always one (1).

Syntax	show monitor sessionsession-id
Command Mode	Privileged EXEC

Parameter	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.
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.

Parameter	Definition
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.

8.18.3. show vlan remote-span

This command displays the configured RSPAN VLAN.

Syntax	show vlan remote-span
Command Mode	Privileged EXEC

8.19. Static MAC Filtering

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.

8.19.1. 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:FF:FF:FF, and FF:FF:FF:FF:FF:FF. The *vlanid* parameter must identify a valid VLAN.

Multicas macfilter adddest function will not affect ip intf.But multicas macfilter addsrc function will affect ip intf.if a physical intf is changed into ip intf,multicas macfilter adddest will not affect ip intf, but you can config macfilter for physical intf and macfilter of the physical intf still exists. when ip intf is changed into physical intf,saved configure will affect physical intf.

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 address MAC address filter with destination ports configured, the maximum number of static filters supported is 512.

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 = 512)
- Multicast MAC and source ports and destination ports (max = 20)

Syntax	macfilter macaddr vlanid
Command Mode	Global Config

8.19.1.1. 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.

Syntax	no macfilter macaddr vlanid
Command Mode	Global Config

8.19.2. 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.

Configuring a destination port list is only valid for multicast MAC addresses.

Syntax	macfilter adddest macaddr
Command Mode	Interface Config

8.19.2.1. 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.

Syntax	no macfilter adddest macaddr
Command Mode	Interface Config

8.19.3. 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.

Configuring a destination port list is only valid for multicast MAC addresses.

Syntax	macfilter adddest all macaddr
Command Mode	Global Config

8.19.3.1. 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.

Syntax	no macfilter adddest all macaddr
Command Mode	Global Config

8.19.4. 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 macaddrand 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.

Syntax	macfilter addsrc macaddr vlanid
Command Mode	Interface Config

8.19.4.1. no macfilter addsrc

This command removes a port from the source filter set for the MAC filter with the MAC address ofmacaddr and VLAN of vlanid. Themacaddr 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.

Syntax	no macfilter addsrc macaddr vlanid
Command Mode	Interface Config

8.19.5. macfilter addsrc all

This command adds all interfaces to the source filter set for the MAC filter with the MAC address of macaddrand 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.

Syntax	macfilter addsrc all macaddr vlanid
Command Mode	Global Config

8.19.5.1. 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 themacaddr 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.

Syntax	no macfilter addsrc all macaddr vlanid
Command Mode	Global Config

8.19.6. 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.

Syntax	show mac-address-table static {macaddr vlanid | all}
Command Mode	Privileged EXEC

Parameter	Definition
MAC Address	The MAC Address of the static MAC filterentry.
VLAN ID	The VLAN ID of the static MAC filter entry.
Source Port(s)	The source port filter set’s slot and port(s).

Only multicast address filters will have destination port lists.

8.19.7. show mac-address-table staticfiltering

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

Syntax show mac-address-table staticfiltering

Command Mode Privileged EXEC

Parameter	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:).

8.20. 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.

8.20.1. 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.

Syntax	dhcp l2relay
Command Mode	Inteface Config / Global Config

8.20.1.1. no dhcp l2relay

This command disables DHCP Layer 2 relay agent for an interface or range of interfaces.

Syntax	no dhcp l2relay
Command Mode	Inteface Config / Global Config

8.20.2. 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.

Syntax	dhcp l2relay circuit-id vlan vlan-list
Command Mode	Global Config
<vlan–list>	The VLAN ID. The range is 1–4093. Separate non-consecutive IDs with a comma (,) no spaces and no zeros in between the range. Use a dash (–) for the range.

8.20.2.1. no dhcp l2relay circuit-id vlan

This parameter clears the DHCP Option-82 Circuit ID for a VLAN.

Syntax	no dhcp l2relay circuit-id vlan vlan-list
Command Mode	Global Config

8.20.3. dhcp l2relay remote-id vlan

This parameter sets the DHCP Option-82 Remote ID for a VLAN and subscribed service (based on subscription- name).

Syntax	dhcp l2relay remote-id remote-id-string vlan vlan-list
Command Mode	Interface Config
<vlan–list>	The VLAN ID. The range is 1–4093. Separate non-consecutive IDs with a comma (,) no spaces and no zeros in between the range. Use a dash (–) for the range.

8.20.3.1. 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).

Syntax	no dhcp l2relay remote-id vlan vlan-list
Command Mode	Interface Config

8.20.4. 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
Syntax	dhcp l2relay vlan vlan-list
Command Mode	Global Config
<vlan–list>	The VLAN ID. The range is 1–4093. Separate non-consecutive IDs with a comma (,) no spaces and no zeros in between the range. Use a dash (–) for the range.

8.20.4.1. no dhcp l2relay vlan

Use this command to disable the DHCP L2 Relay agent for a set of VLANs.

Syntax	no dhcp l2relay vlan vlan-list
Command Mode	Global Config

8.20.5. dhcp l2relay trust

Use this command to configure an interface or range of interfaces as trusted for Option-82 reception.

Default	untrusted
Syntax	dhcp l2relay trust
Command Mode	Interface Config

8.20.5.1. no dhcp l2relay trust

Use this command to configure an interface to the default untrusted for Option-82 reception.

Syntax	no dhcp l2relay trust
Command Mode	Interface Config

8.20.6. show dhcp l2relay all

This command displays the summary of DHCP L2 Relay configuration.

Syntax	show dhcp l2relay all
Command Mode	Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(Switching) #show dhcp l2relay all
```

```
DHCP L2 Relay is Enabled.
Interface  L2RelayMode TrustMode
---------- ----------- --------------
1/0/2      Enabled     untrusted
1/0/4      Disabled    trusted
```

```
VLAN Id   L2 Relay   CircuitId   RemoteId
--------- ---------- ----------- ------------
3         Disabled   Enabled     --NULL--
5         Enabled    Enabled     --NULL--
6         Enabled    Enabled     FASTPATH
7         Enabled    Disabled    --NULL--
8         Enabled    Disabled    --NULL--
9         Enabled    Disabled    --NULL--
10        Enabled    Disabled    --NULL--
```

8.20.7. show dhcp l2relay circuit-id vlan

This command displays DHCP circuit-id vlan configuration.

Syntax	show dhcp l2relay circuit-id vlan vlan-list
Command Mode	Privileged EXEC
<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.

8.20.8. show dhcp l2relay interface

This command displays DHCP L2 relay configuration specific to interfaces.

Syntax	show dhcp l2relay interface {all | interface-num}
Command Mode	Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(Switching) #show dhcp l2relay interface all
```

```
DHCP L2 Relay is Enabled.
Interface  L2RelayMode TrustMode
---------- ----------- --------------
0/2        Enabled     untrusted
0/4        Disabled    trusted
```

8.20.9. show dhcp l2relay remote-id vlan

This command displays DHCP Remote-id vlan configuration.

Syntax	show dhcp l2relay remote-id vlan vlan-list
Command Mode	Privileged EXEC
<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.

8.20.10. show dhcp l2relay stats interface

This command displays statistics specific to DHCP L2 Relay configured interface.

Syntax	show dhcp l2relay stats interface {all | interface-num}
Command Mode	Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(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
```

8.20.11. show dhcp l2relay agent-option vlan

This command displays the DHCP L2 Relay Option-82 configuration specific to VLAN.

Syntax	show dhcp l2relay agent-option vlan vlan-range
Command Mode	Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(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    FASTPATH
7         Enabled    Disabled   --NULL--
8         Enabled    Disabled   --NULL--
9         Enabled    Disabled   --NULL--
10        Enabled    Disabled   --NULL--
```

8.20.12. show dhcp l2relay vlan

This command displays DHCP vlan configuration.

Syntax	show dhcp l2relay vlan vlan-list
Command Mode	Privileged EXEC
<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.

8.20.13. 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.

Syntax	clear dhcp l2relay statistics interface { unit/slot/port | all }
Command Mode	Privileged EXEC

8.21. IGMP Snooping Configuration Commands

This section describes the commands you use to configure IGMP snooping. FASTPATH 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.

This note clarifies the prioritization of MGMD Snooping Configurations. Many of the IGMP 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.

8.21.1. 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 reenabled 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
Syntax	set igmp [vlan_id]
Command Mode	Global Config / Interface Config / VLAN Config

8.21.1.1. no set igmp

This command disables IGMP Snooping on the system, an interface, a range of interfaces, or a VLAN.

Syntax	no set igmp [vlan_id]
Command Mode	Global Config / Interface Config / VLAN Config

8.21.2. 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 reenabled if you disable routing or remove port-channel (LAG) membership from an interface that has IGMP Snooping enabled.

Default	disabled
Syntax	set igmp interfacemode
Command Mode	Global Config

8.21.2.1. no set igmp interfacemode

This command disables IGMP Snooping on all interfaces.

Syntax	no set igmp interfacemode
Command Mode	Global Config

8.21.3. 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 remove immediately the Layer 2 LAN interface from its forwarding table entry upon receiving an IGMP leave a 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
Syntax	set igmp fast-leave[vlan_id]
Command Mode	Global Config / Interface Config / VLAN Config

8.21.3.1. no set igmp fast-leave

This command disables IGMP Snooping fast-leave admin mode on a selected interface.

Syntax	no set igmp fast-leave [vlan_id]
Command Mode	Global Config / Interface Config / VLAN Config

8.21.4. 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
Syntax	set igmp groupmembership-interval [vlan_id] 2-3600
Command Mode	Global Config / Interface Config / VLAN Config

8.21.4.1. no set igmp groupmembership-interval

This command sets the IGMPv3 Group Membership Interval time to the default value.

Syntax	no set igmp groupmembership-interval [vlan_id]
Command Mode	Global Config / Interface Config / VLAN Config

8.21.5. 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
Syntax	set igmp maxresponse [vlan_id] 1-25
Command Mode	Global Config / Interface Config / VLAN Config

8.21.5.1. no set igmp maxresponse

This command sets the max response time (on the interface or VLAN) to the default value.

Syntax	no set igmp maxresponse [vlan_id]
Command Mode	Global Config / Interface Config / VLAN Config

8.21.6. 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
Syntax	set igmp mcrtrexpiretime [vlan_id] 0-3600
Command Mode	Global Config / Interface Config / VLAN Config

8.21.6.1. 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.

Syntax	no set igmp mcrtrexpiretime[vlan_id]
Command Mode	Global Config / Interface Config / VLAN Config

8.21.7. set igmp mrouter

This command configures the VLAN ID (vlan_id) that has the multicast router mode enabled.

Syntax	set igmp mrouter vlan_id
Command Mode	Interface Config

8.21.7.1. no set igmp mrouter

This command disables multicast router mode for a particular VLAN ID (vlan_id).

Syntax	no set igmp mrouter vlan_id
Command Mode	Interface Config

8.21.8. 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
Syntax	set igmp mrouter interface
Command Mode	Interface Config

8.21.8.1. no set igmp mrouter interface

This command disables the status of the interface as a statically configured multicast router interface.

Syntax	no set igmp mrouter interface
Command Mode	Interface Config

8.21.9. 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
Syntax	set igmp report-suppression vlan-id
Command Mode	VLAN Config
<vlan-id>	A valid VLAN ID. Range is 1 to 4093.

Example: The following shows an example of the command.

```
(Routing) #vlan database
(Routing) (Vlan)#set igmp report-suppression 1
```

8.21.9.1. no set igmp report-suppression

Use this command to return the system to the default.

Syntax	no set igmp report-suppression
Command Mode	VLAN Config

8.21.10. show igmpsnooping

This command displays IGMP Snooping information for a given *unit/slot/port* or VLAN. Configured information is displayed whether or not IGMP Snooping is enabled.

Syntax	show igmpsnooping [unit/slot/port | vlan_id]
Command Mode	Privileged EXEC

When the optional arguments *unit/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.

Term	Definition
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 *unit/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	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 beconfigured.
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.
Report SuppressionMode	Indicates whether IGMP reports (set by the command **set igmp report-suppression**) in enabled or not.

Example: The following shows example CLI display output for the command.

```
(Routing) #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
```

8.21.11. show igmpsnooping mrouter interface

This command displays information about statically configured ports.

Syntax	show igmpsnooping mrouter interface unit/slot/port
Command Mode	Privileged EXEC

Term	Definition
Interface	The port on which multicast router information is being displayed.
Multicast Router Attached	Indicates whether multicast router is statically enabled on the interface.
VLAN ID	The list of VLANs of which the interface is a member.

8.21.12. show igmpsnooping mrouter vlan

This command displays information about statically configured ports.

Syntax	show igmpsnooping mrouter vlan unit/slot/port
Command 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.

8.21.13. 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.

Syntax	show igmpsnooping ssm {entries | groups | stats}
Command Mode	Privileged EXEC

8.21.14. show mac-address-table igmpsnooping

This command displays the IGMP Snooping entries in the MFDB table.

Syntax show mac-address-table igmpsnooping

Command 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:).

8.22. 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 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.

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.

8.22.1. 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 reenabled if IGMP Snooping is operational on the VLAN.

The Querier IP Address assigned to 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
Syntax	set igmp querier [vlan-id] [address ipv4_address]
Command Mode	Global Config / VLAN Mode

8.22.1.1. 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.

Syntax	no set igmp querier [vlan-id] [address]
Command Mode	Global Config / VLAN Mode

8.22.2. 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
Syntax	set igmp querier query-interval 1-1800
Command Mode	Global Config

8.22.2.1. no set igmp querier query-interval

Use this command to set the IGMP Querier Query Interval time to its default value.

Syntax	no set igmp querier query-interval
Command Mode	Global Config

8.22.3. 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	125 seconds
Syntax	set igmp querier timer expiry 60-300
Command Mode	Global Config

8.22.3.1. no set igmp querier timer expiry

Use this command to set the IGMP Querier timer expiration period to its default value.

Syntax	no set igmp querier timer expiry
Command Mode	Global Config

8.22.4. 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	2
Syntax	set igmp querier version 1-2
Command Mode	Global Config

8.22.4.1. no set igmp querier version

Use this command to set the IGMP Querier version to its default value.

Syntax	no set igmp querier version
Command Mode	Global Config

8.22.5. 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 Queriersending periodic queries. If the Snooping Querier wins the election, then it will continue sending periodic queries.

Default	disabled
Syntax	set igmp querier election participate
Command Mode	VLAN Config

8.22.5.1. 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.

Syntax	no set igmp querier election participate
Command Mode	VLAN Config

8.22.6. show igmpsnooping querier

Use this command to display IGMP Snooping Querier information. Configured information is displayed whether or not IGMP Snooping Querier is enabled.

Syntax	show igmpsnooping querier [{detail | vlan vlanid}]
Command Mode	Privileged EXEC

When the optional argument *vlanid* is not used, the command displays the following information.

Field	Definition
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.

Field	Definition
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	Definition
VLAN Admin Mode	Indicates whether iGMP Snooping Querier is active on the VLAN.
VLAN Operational State	Indicates whether IGMP Snooping Querier is in. 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 outany queries.
VLAN Operational Max Response Timea	Indicates the time to wait before removing a host upon receiving 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.

8.23. 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.

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.

8.23.1. 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
Syntax	set mld vlanid
Command Mode	Global Config / Interface Config / VLAN Mode

8.23.1.1. no set mld

Use this command to disable MLD Snooping on the system.

Syntax	set mld vlanid
Command Mode	Global Config / Interface Config / VLAN Mode

8.23.2. 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
Syntax	set mld interfacemode
Command Mode	Global Config

8.23.2.1. no set mld interfacemode

Use this command to disable MLD Snooping on all interfaces.

Syntax	no set mld interfacemode
Command Mode	Global Config

8.23.3. 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.

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.

Fast-leave processing is supported only with MLD version 1 hosts.

Default	disabled
Syntax	set mld fast-leave vlanid
Command Mode	Interface Config / VLAN Mode

8.23.3.1. no set mld fast-leave

Use this command to disable MLD Snooping fast-leave admin mode on a selected interface.

Syntax	no set mld fast-leave vlanid
Command Mode	Interface Config / VLAN Mode

8.23.4. 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
Syntax	set mld groupmembership-interval vlanid 2-3600
Command Mode	Interface Config / VLAN Mode

8.23.4.1. no set groupmembership-interval

Use this command to set the MLDv2 Group Membership Interval time to the default value.

Syntax	no set mld groupmembership-interval
Command Mode	Interface Config / VLAN Mode

8.23.5. 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
Syntax	set mld maxresponse 1-65
Command Mode	Global Config / Interface Config / VLAN Mode

8.23.5.1. no set mld maxresponse

Use this command to set the max response time (on the interface or VLAN) to the default value.

Syntax	no set mld maxresponse
Command Mode	Global Config / Interface Config / VLAN Mode

8.23.6. 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
Syntax	set mld mcrtexpiretime vlanid 0-3600
Command Mode	Global Config / Interface Config / VLAN Mode

8.23.6.1. 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.

Syntax	no set mld mcrtexpiretime vlanid
Command Mode	Global Config / Interface Config / VLAN Mode

8.23.7. set mld mrouter

Use this command to configure the VLAN ID for the VLAN that has the multicast router attached mode enabled.

Syntax	set mld mrouter vlanid
Command Mode	Global Config / Interface Config

8.23.7.1. no set mld mrouter

Use this command to disable multicast router attached mode for a VLAN with a particular VLAN ID.

Syntax	no set mld mrouter vlanid
Command Mode	Global Config / Interface Config

8.23.8. 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
Syntax	set mld mrouter interface
Command Mode	Interface Config

8.23.8.1. no set mld mrouter interface

Use this command to disable the status of the interface as a statically configured multicast router-attached interface.

Syntax	no set mld mrouter interface
Command Mode	Interface Config

8.23.9. show mldsnooping

Use this command to display MLD Snooping information. Configured information is displayed whether or not MLD Snooping is enabled.

Syntax	show mldsnooping [unit/slot/port | vlanid]
Command 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.
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
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.

8.23.10. show mldsnooping mrouter interface

Use this command to display information about statically configured multicast router attached interfaces.

Syntax show mldsnooping mrouter interface unit/slot/port

Command 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.
VLAN ID	Displays the list of VLANs of which the interface is a member.

8.23.11. show mldsnooping mrouter vlan

Use this command to display information about statically configured multicast router-attached interfaces.

Syntax show mldsnooping mrouter vlan unit/slot/port

Command 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.

8.23.12. show mldsnooping ssm entries

Use this command to display the source specific multicast forwarding database built by MLD snooping.

Syntax show mldsnooping ssm entries

Command Mode Privileged EXEC

Term	Definition
VLAN	The VLAN on which the entry is learned.

Term	Definition
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.

8.23.13. show mldsnooping ssm stats

Use this command to display the statistics of MLD snooping

Syntax show mldsnooping ssm stats

Command Mode Privileged EXEC

Term	Definition
Total Entries	The total number of entries that can possibly be in the MLD snooping
Most SSMFDB Entries Ever Used	The largest number of entries that have been present in the MLD snooping
Current Entries	The current number of entries in the MLD snooping

8.23.14. show mldsnooping ssm groups

Use this command to display the MLD SSM group membership information.

Syntax show mldsnooping ssm groups

Command 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.

Term	Definition
Source Address List	List of source IP addresses for which source filtering is requested.

8.23.15. show mac-address-table mldsnooping

Use this command to display the MLD Snooping entries in the Multicast Forwarding Database (MFDB) table.

Syntax show mac-address-table mldsnooping

Command 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:).

8.23.16. clear mldsnooping

Use this command to delete all MLD snooping entries from the MFDB table.

Syntax clear mldsnooping

Command Mode Privileged EXEC

8.24. 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.

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.

8.24.1. set mld querier

Use this command to enable MLD Snooping Querier on the system (Global Config Mode) or 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
Syntax	set mld querier [vlan-id] [address ipv6_address]
Command Mode	Global Config / VLAN Mode

8.24.1.1. 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.

Syntax	no set mld querier [vlan-id][address]
Command Mode	Global Config / VLAN Mode

8.24.2. 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
Syntax	set mld querier query_interval 1-1800
Command Mode	Global Config

8.24.2.1. no set mld querier query_interval

Use this command to set the MLD Querier Query Interval time to its default value.

Syntax	no set mld querier query_interval
Command Mode	Global Config

8.24.3. 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
Syntax	set mld querier timer expiry 60-300
Command Mode	Global Config

8.24.3.1. no set mld querier timer expiry

Use this command to set the MLD Querier timer expiration period to its default value.

Syntax	no set mld querier timer expiry
Command Mode	Global Config

8.24.4. 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 Queriersending periodic queries. If the Snooping Querier wins the election, then it will continue sending periodic queries.

Default	disabled
Syntax	set mld querier election participate
Command Mode	VLAN Config

8.24.4.1. 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.

Syntax	no set mld querier election participate
Command Mode	VLAN Config

8.24.5. show mldsnooping querier

Use this command to display MLD Snooping Querier information. Configured information is displayed whether or not MLD Snooping Querier is enabled.

Syntax	show mldsnooping querier [{detail | vlan vlanid}]
Command 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 VLAN 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 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.

Field	Description
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.

8.25. 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.

Port-security function only supports PHYSICAL INTF and LAG INTF. If a physical intf is changed into ip intf, port-security will not affect ip intf, but you can config port-security for physical intf and port-security configure of the physical intf still exists. When ip intf is changed into physical intf, saved configure will affect physical intf.

Port-security can cause partner's designated port changing port state from forwarding to discarding because of root port cannot receive BPDU sended by a partner. It is a normal phenomenon. If you add STP BPDU src mac into port-security static table, the Discarding status will be changed into forward status.

Use port-security add port channel's mac: when a port channel is up, show mac-addr-table will show *learning*; when a port channel is down, show mac-addr-table will show *static*.

8.25.1. port-security

This command enables port locking on an interface, a range of interfaces, or at the system level.

Default	disabled
Syntax	port-security
Command Mode	Interface Config (to enable port locking on an interface or range of interfaces) / Global Config (to enable port locking globally)

8.25.1.1. no port-security

This command disables port locking for one (Interface Config) or all (Global Config) ports.

Syntax	no port-security
Command Mode	Interface Config / Global Config

8.25.2. port-security max-dynamic

This command sets the maximum number of dynamically locked MAC addresses allowed on a specific port.

Default	600
Syntax	port-security max-dynamic maxvalue
Command Mode	Interface Config

8.25.2.1. 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.

Syntax	no port-security max-dynamic
Command Mode	Interface Config

8.25.3. port-security max-static

This command sets the maximum number of statically locked MAC addresses allowed on a port.

Default	20
Syntax	port-security max-static maxvalue
Command Mode	Interface Config

8.25.3.1. no port-security max-static

This command sets maximum number of statically locked MAC addresses to the default value.

Syntax	no port-security max-static
Command Mode	Interface Config

8.25.4. 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.

Syntax	port-security mac-address mac-address vid
Command Mode	Interface Config

8.25.4.1. no port-security mac-address

This command removes a MAC address from the list of statically locked MAC addresses.

Syntax	no port-security mac-address mac-address vid
Command Mode	Interface Config

8.25.5. port-security mac-address move

This command converts dynamically locked MAC addresses to statically locked addresses for an interface or range of interfaces.

Syntax	port-security mac-address move
Command Mode	Interface Config

8.25.6. show port-security

This command displays the port-security settings. If you do not use a parameter, the command displays the settings for the entire system. Use the optional parameters to display the settings on a specific interface or on all interfaces.

Syntax	show port-security [{ unit/slot/port | lag lag-id | all }]
Command 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.

8.25.7. show port-security dynamic

This command displays the dynamically locked MAC addresses for the port.

Syntax	show port-security dynamic { unit/slot/port | lag lag-id }
Command Mode	Privileged EXEC

Term	Definition
MAC Address	MAC Address of dynamically locked MAC.

8.25.8. show port-security static

This command displays the statically locked MAC addresses for port.

Syntax	show port-security static { unit/slot/port | lag lag-id }
Command Mode	Privileged EXEC

Term	Definition
MAC Address	MAC Address of statically locked MAC

8.25.9. show port-security violation

This command displays the source MAC address of the last packet discarded on a locked port.

Syntax show port-security violation { unit/slot/port | lag lag-id }

Command Mode Privileged EXEC

Term	Definition
MAC Address	MAC Address of statically locked MAC.

8.26. 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.

8.26.1. lldp transmit

Use this command to enable the LLDP advertise capability on an interface or a range of interfaces.

Default	disabled
Syntax	lldp transmit
Command Mode	Interface Config

8.26.1.1. no lldp transmit

Use this command to return the local data transmission capability to the default.

Syntax	no lldp transmit
Command Mode	Interface Config

8.26.2. lldp receive

Use this command to enable the LLDP receive capability on an interface or a range of interfaces.

Default	disabled
Syntax	lldp receive
Command Mode	Interface Config

8.26.2.1. no lldp receive

Use this command to return the reception of LLDPDUs to the default value.

Syntax	no lldp receive
Command Mode	Interface Config

8.26.3. 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 1-10 seconds.

Default	interval-30 seconds / hold-4 / reinit-2 seconds
Syntax	lldp timers [interval interval-seconds] [hold hold-value] [reinit reinit-seconds]
Command Mode	Global Config

8.26.3.1. 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.

Syntax	no lldp timers [interval] [hold] [reinit]
Command Mode	Global Config

8.26.4. 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. 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.

Default	no optional TLVs are included
Syntax	lldp transmit-tlv [sys-desc] [sys-name] [sys-cap] [port-desc]
Command Mode	Interface Config

8.26.4.1. 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.

Syntax	no lldp transmit-tlv [sys-desc] [sys-name] [sys-cap] [port-desc]
Command Mode	Interface Config

8.26.5. lldp transmit-mgmt

Use this command to include transmission of the local system management address information in the LLDPDUs. This command ca be used to configure a single interface or a range of interfaces.

Syntax	lldp transmit-mgmt

Command Mode	Interface Config

8.26.5.1. 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.

Syntax	no lldp transmit-mgmt
Command Mode	Interface Config

8.26.6. lldp notification

Use this command to enable remote data change notifications on an interface or a range of interfaces.

Default	disabled
Syntax	lldp notification
Command Mode	Interface Config

8.26.6.1. no lldp notification

Use this command to disable notifications.

Default	disabled
Syntax	no lldp notification
Command Mode	Interface Config

8.26.7. 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
Syntax	lldp notification-interval interval
Command Mode	Global Config

8.26.7.1. no lldp notification-interval

Use this command to return the notification interval to the default value.

Syntax	no lldp notification-interval

Command Mode	Global Config

8.26.8. clear lldp statistics

Use this command to reset all LLDP statistics, including MED-relatedinformation.

Syntax	clear lldp statistics
Command Mode	Privileged EXEC

8.26.9. clear lldp remote-data

Use this command to delete all information from the LLDP remote data table, including MED-related information.

Syntax	clear lldp remote-data
Command Mode	Global Config

8.26.10. show lldp

Use this command to display a summary of the current LLDP configuration.

Syntax	show lldp
Command Mode	Privileged EXEC

Parameter	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

8.26.11. show lldp interface

Use this command to display a summary of the current LLDP configuration for a specific interface or for all interfaces.

Syntax	show lldp interface {unit/slot/port | all}
Command Mode	Privileged EXEC

Parameter	Definition
Interface	The interface in a unit/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.
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.

8.26.12. show lldp statistics

Use this command to display the current LLDP traffic and remote table statistics for a specific interface or for all interfaces.

Syntax show lldp statistics {unit/unit/slot/port | all}

Command 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.
TotalDrops	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 unit/unit/slot/port
Transmit Total	Total number of LLDP packets transmitted on the port.
Receive 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.

Term	Definition
TVLUnknowns	Total number of LLDP TLVs received on the port where the type value is in the reserved range, and not recognized.

8.26.13. 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.

Syntax	show lldp remote-device {unit/unit/slot/port | all}
Command 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.

Example: The following shows example CLI display output for the command.

```
(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
```

8.26.14. 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.

Syntax	show lldp remote-device detail unit/unit/slot/port
Command 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.
Port ID	The port number that transmitted the LLDPDU.
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 a 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.
ManagementAddress	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.
Time To Live	The amount of time (in seconds) the remote device's information received in the LLDPDU should be treated as valid information.

Example: The following shows example CLI display output for the command.

```
(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
```

8.26.15. 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.

Syntax	show lldp local-device {unit/unit/slot/port | all}
Command Mode	Privileged EXEC

Term	Definition
Interface	The interface in a unit/unit/slot/port format.
Port ID	The port ID associated with this interface.
Port Description	The port description associated with the interface.

8.26.16. show lldp local-device detail

Use this command to display detailed information about the LLDP data a specific interface transmits.

Syntax	show lldp local-device detail unit/unit/slot/port
Command 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 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 a 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.
ManagementAddress	The type of address and the specific address the local LLDP agent uses to send and receive information.

8.27. 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.

8.27.1. 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
Syntax	lldp med
Command Mode	Interface Config

8.27.1.1. no lldp med

Use this command to disable MED.

Syntax	no lldp med
Command Mode	Interface Config

8.27.2. lldp med confignotification

Use this command to configure an interface or a range of interfaces to send the topology change notification.

Default	disabled
Syntax	lldp med confignotification
Command Mode	Interface Config

8.27.2.1. no lldp med confignotification

Use this command to disable notifications.

Syntax	no lldp med confignotification
Command Mode	Interface Config

8.27.3. 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.
Syntax	lldp med transmit-tlv [capabilities] [ex-pd] [ex-pse] [inventory] [location] [network-policy]
Command Mode	Interface Config
<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

8.27.3.1. no lldp med transmit-tlv

Use this command to remove a TLV.

Syntax	no lldp med transmit-tlv [network-policy]
Command Mode	Interface Config

8.27.4. lldp med all

Use this command to configure LLDP-MED on all the ports.

Syntax	lldp med all
Command Mode	Global Config

8.27.5. lldp med confignotification all

Use this command to configure all the ports to send the topology change notification.

Syntax	lldp med confignotification all
Command Mode	Global Config

8.27.6. 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
Syntax	lldp med faststartrepeatcount [count]
Command Mode	Global Config

8.27.6.1. no lldp med faststartrepeatcount

Use this command to return to the factory default value.

Syntax	no lldp med faststartrepeatcount
Command Mode	Global Config

8.27.7. 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.
Syntax	lldp med transmit-tlv all [capabilities] [ex-pd] [ex-pse] [inventory] [location] [network-policy]
Command Mode	Global Config
<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.

8.27.7.1. no lldp med transmit-tlv all

Use this command to remove a TLV.

Syntax	no lldp med transmit-tlvall [network-policy]
Command Mode	Global Config

8.27.8. show lldp med

Use this command to display a summary of the current LLDP MED configuration.

Syntax	show lldp med
Command Mode	Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(Routing) #show lldp med
LLDP MED Global Configuration
```

```
Fast Start Repeat Count: 3
Device Class: Network Connectivity
(Routing) #
```

8.27.9. show lldp med local-device detail

Use this command to display detailed information about the LLDP MED data that a specific interface transmits.

unit/slot/port indicates a specific physical interface.

Syntax	show lldp med local-device detail unit/slot/port
Command Mode	Privileged EXEC

8.27.10. 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.

Syntax	show lldp med remote-device {unit/slot/port | all}
Command 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.

Example: The following shows example CLI display output for the command.

```
(Routing) #show lldp med remote-device all
LLDP MED Remote Device Summary
Local
Interface Remote ID Device Class
--------- --------- ------------
1/0/8     1         Class I
1/0/9     2         Not Defined
1/0/10    3         Class II
1/0/11    4         Class III
1/0/12    5         Network Co
```

8.27.11. 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.

Syntax	show lldp med remote-device detail unit/unit/slot/port
Command Mode	Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(Espada) #show lldp med local-device detail 0/8
LLDP MED Local Device Detail

Interface: 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
```

8.28. 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: IP Header size smaller than configured value.#drop the packet which must be the first fragment and (packet length in IP header)–20 < Minimum TCP header size.#
- TCP Fragment: IP Fragment Offset = 1 and IP Header size smaller than configured value. But it can’t modify value of the Min TCP Hdr Size. If you want to modify the value, please use "dos-control firstfrag value"
- 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.

Monitoring and blocking of the types of attacks listed below are only supported on the BCM56538, BCM56840, BCM56843, BCM56845, BCM56846, and BCM5685x platforms.

- 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:IP Fragment Offset = 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.

8.28.1. dos-control all

This command enables Denial of Service protection checks globally.

Default	disabled
Syntax	dos-control all
Command Mode	Global Config

8.28.1.1. no dos-control all

This command disables Denial of Service prevention checks globally.

Syntax	no dos-control all
Command Mode	Global Config

8.28.2. 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
Syntax	dos-control sipdip
Command Mode	Global Config

8.28.2.1. no dos-control sipdip

This command disables Source IP address = Destination IP address (SIP = DIP) Denial of Service prevention.

Syntax	no dos-control sipdip
Command Mode	Global Config

8.28.3. 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)
Syntax	dos-control firstfrag [0-255]
Command Mode	Global Config

8.28.3.1. no dos-control firstfrag

This command sets Minimum TCP Header Size Denial of Service protection to the default value of *disabled*.

Syntax	no dos-control firstfrag
Command Mode	Global Config

8.28.4. 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. If packets ingress having IP Fragment Offset equal to one (1), the packets will be dropped if the mode is enabled.

Default	disabled
Syntax	dos-control tcpfrag
Command Mode	Global Config

8.28.4.1. no dos-control tcpfrag

This command disabled TCP Fragment Denial of Service protection.

Syntax	no dos-control tcpfrag
Command Mode	Global Config

8.28.5. 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 and packets will be dropped, as follows:

- Packets ingress have the TCP Flag SYN set and a source port less than 1024.
- The TCP Control Flags are set to 0 and the TCP Sequence Number is set to 0.
- The TCP Flags FIN, URG, and PSH are set and the TCP Sequence Number is set to 0.
- The TCP Flags SYN and FIN are both set.

Default	disabled
Syntax	dos-control tcpflag
Command Mode	Global Config

8.28.5.1. no dos-control tcpflag

This command sets disables TCP Flag Denial of Service protections.

Syntax	no dos-control tcpflag
Command Mode	Global Config

8.28.6. 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.

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
Syntax	dos-control l4port
Command Mode	Global Config

8.28.6.1. no dos-control l4port

This command disables L4 Port Denial of Service protections.

Syntax	no dos-control l4port
Command Mode	Global Config

8.28.7. dos-control icmp

This command enables Maximum ICMP Packet Size Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attack. If ICMP 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)
Syntax	dos-control icmp 0-1023
Command Mode	Global Config

8.28.7.1. no dos-control icmp

This command disables Maximum ICMP Packet Size Denial of Service protections.

Syntax	no dos-control icmp

Command Mode	Global Config

8.28.8. dos-control smacdmac

This command is only supported on the BCM56538, BCM56840, BCM56843, BCM56845, BCM56846, and BCM5685x platforms.

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
Syntax	dos-control smacdmac
Command Mode	Global Config

8.28.8.1. no dos-control smacdmac

This command disables Source MAC address = Destination MAC address (SMAC = DMAC) DoS protection.

Syntax	no dos-control smacdmac
Command Mode	Global Config

8.28.9. dos-control tcpport

This command is only supported on the BCM56538, BCM56840, BCM56843, BCM56845, BCM56846, and BCM5685x platforms.

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
Syntax	dos-control tcpport
Command Mode	Global Config

8.28.9.1. no dos-control tcpport

This command disables TCP L4 source = destination port number (Source TCP Port = Destination TCP Port) Denial of Service protection.

Syntax	no dos-control smacdmac
Command Mode	Global Config

8.28.10. dos-control udpport

This command is only supported on the BCM56538, BCM56840, BCM56843, BCM56845, BCM56846, and BCM5685x platforms.

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
Syntax	dos-control udpport
Command Mode	Global Config

8.28.10.1. no dos-control udpport

This command disables UDP L4 source = destination port number (Source UDP Port = Destination UDP Port) Denial of Service protection.

Syntax	no dos-control udpport
Command Mode	Global Config

8.28.11. dos-control tcpflagseq

This command is only supported on the BCM56538, BCM56840, BCM56843, BCM56845, BCM56846, and BCM5685x platforms.

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
Syntax	dos-control tcpflagseq
Command Mode	Global Config

8.28.11.1. no dos-control tcpflagseq

This command sets disables TCP Flag and Sequence Denial of Service protection.

Syntax	no dos-control tcpflagseq
Command Mode	Global Config

8.28.12. dos-control tcpoffset

This command is only supported on the BCM56538, BCM56840, BCM56843, BCM56845, BCM56846, and BCM5685x platforms.

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
Syntax	dos-control tcpoffset
Command Mode	Global Config

8.28.12.1. no dos-control tcpoffset

This command disabled TCP Offset Denial of Service protection.

Syntax	no dos-control tcpoffset
Command Mode	Global Config

8.28.13. dos-control tcpsyn

This command is only supported on the BCM56538, BCM56840, BCM56843, BCM56845, BCM56846, and BCM5685x platforms.

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
Syntax	dos-control tcpsyn
Command Mode	Global Config

8.28.13.1. no dos-control tcpsyn

This command sets disables TCP SYN and L4 source = 0-1023 Denial of Service protection.

Syntax	no dos-control tcpsyn
Command Mode	Global Config

8.28.14. dos-control tcpsynfin

This command is only supported on the BCM56538, BCM56840, BCM56843, BCM56845, BCM56846, and BCM5685x platforms.

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
Syntax	dos-control tcpsynfin
Command Mode	Global Config

8.28.14.1. no dos-control tcpsynfin

This command sets disables TCP SYN & FIN Denial of Service protection.

Syntax	no dos-control tcpsynfin
Command Mode	Global Config

8.28.15. dos-control tcpfinurgpsh

This command is only supported on the BCM56538, BCM56840, BCM56843, BCM56845, BCM56846, and BCM5685x platforms.

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

Syntax: dos-control tcpfinurgpsh

Command Mode
Global Config

8.28.15.1. no dos-control tcpfinurgpsh

This command sets disables TCP FIN and URG and PSH and SEQ = 0 checking Denial of Service protections.

Syntax	no dos-control tcpfinurgpsh
Command Mode	Global Config

8.28.16. dos-control icmpv4

This command is only supported on the BCM56538, BCM56840, BCM56843, BCM56845, BCM56846, and BCM5685x platforms.

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)
Syntax	dos-control icmpv4 0-16384
Command Mode	Global Config

8.28.16.1. no dos-control icmpv4

This command disables Maximum ICMP Packet Size Denial of Service protections.

Syntax	no dos-control icmpv4
Command Mode	Global Config

8.28.17. dos-control icmpv6

This command is only supported on the BCM56538, BCM56840, BCM56843, BCM56845, BCM56846, and BCM5685x platforms.

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)
Syntax	dos-control icmpv6 0-16384
Command Mode	Global Config

8.28.17.1. no dos-control icmpv6

This command disables Maximum ICMP Packet Size Denial of Service protections.

Syntax	no dos-control icmpv6
Command Mode	Global Config

8.28.18. dos-control icmpfrag

This command is only supported on the BCM56538, BCM56840, BCM56843, BCM56845, BCM56846, and BCM5685x platforms.

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
Syntax	dos-control icmpfrag
Command Mode	Global Config

8.28.18.1. no dos-control icmpfrag

This command disabled ICMP Fragment Denial of Service protection.

Syntax	no dos-control icmpfrag
Command Mode	Global Config

8.28.19. show dos-control

This command displays Denial of Service configuration information.

Syntax	show dos-control
Command Mode	Privileged EXEC

Some of the information below displays only if you are using the BCM56538, BCM56840, BCM56843, BCM56845, BCM56846, and BCM5685x platforms.

Term	Definition
First Fragment Mode	May be enabled or disabled. The factory default is disabled.
Min TCP Hdr Size <0-255>	The factory default is 20.

Term	Definition
ICMP Mode	May be enabled or disabled. The factory default is disabled.
Max ICMPv4 Pkt Size	The range is 0-1023. The factory default is 512.
Max ICMPv6 Pkt Size	The range is 0-16384. The factory default is 512.
ICMP Fragment Mode	May be enabled or disabled. The factory default is disabled.
L4 Port Mode	May be enabled or disabled. The factory default is disabled.
TCP Port Mode	May be enabled or disabled. The factory default is disabled.
UDP Port Mode	May be enabled or disabled. The factory default is disabled.
SIPDIP Mode	May be enabled or disabled. The factory default is disabled.
SMACDMAC Mode	May be enabled or disabled. The factory default is disabled.
TCP Flag Mode	May be enabled or disabled. The factory default is disabled.
TCP FIN&URG& PSH Mode	May be enabled or disabled. The factory default is disabled.
TCP Flag & Sequence Mode	May be enabled or disabled. The factory default is disabled.
TCP SYN Mode	May be enabled or disabled. The factory default is disabled.
TCP SYN & FIN Mode	May be enabled or disabled. The factory default is disabled.
TCP Fragment Mode	May be enabled or disabled. The factory default is disabled.
TCP Offset Mode	May be enabled or disabled. The factory default is disabled.

8.29. MAC Database Commands

This section describes the commands you use to configure and view information about the MAC databases.

8.29.1. 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.

Default	300
Syntax	bridge aging-time 10-1,000,000
Command Mode	Global Config

8.29.1.1. no bridge aging-time

This command sets the forwarding database address aging timeout to the default value.

Syntax	no bridge aging-time
Command Mode	Global Config

8.29.2. show forwardingdb agetime

This command displays the timeout for address aging.

Default	all
Syntax	show forwardingdb agetime
Command Mode	Privileged EXEC

Term	Definition
Address Aging Timeout	Displays the system’s address aging timeout value in seconds.

8.29.3. 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.

Syntax	show mac-address-table multicast macaddr
Command 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.
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.
Component	The component that is responsible for this entry in the Multicast Forwarding Database. Possible values are IGMP Snooping, GMRP, and Static Filtering.
Description	The text description of this multicast table entry.
Interfaces	The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).
Forwarding Interfaces	The resultant forwarding list is derived from combining all the component interfaces and removing the interfaces that are listed as the static filtering interfaces.

8.29.4. show mac-address-table stats

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

Syntax show mac-address-table stats

Command 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 Entries Ever Used table. This value is also known as the MFDB high-water mark.
Current Entries	The current number of entries in the MFDB.

Chapter 9. Routing Commands

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

The Routing Commands chapter contains the following sections:

9.1. Address Resolution Protocol Commands

This section describes the commands you use to configure Address Resolution Protocol (ARP) and to view ARP information on the switch. ARP associates IP addresses with MAC addresses and stores the information as ARP entries in the ARP cache.

9.1.1. arp

This command creates an ARP entry. The value for *ipaddress* is the IP address of a device on a subnet attached to an existing routing interface. The parameter *macaddr* is a unicast MAC address for that device.

The format of the MAC address is 6 two-digit hexadecimal numbers that are separated by colons, for example, 00:06:29:32:81:40.

Syntax	arp ipaddress macaddr
Command Mode	Global Config

9.1.1.1. no arp

This command deletes an ARP entry. The value for *arpentry* is the IP address of the interface. The value for *ipaddress* is the IP address of a device on a subnet attached to an existing routing interface. The parameter *macaddr* is a unicast MAC address for that device.

Syntax	no arp ipaddress macaddr
Command Mode	Global Config

9.1.2. arp cachesize

This command configures the ARP cache size. The ARP cache size value is a platform-specific integer value. The default size also varies depending on the platform.

Syntax	arp cachesize platform specific integer value
Command Mode	Global Config

9.1.2.1. no arp cachesize

This command configures the default ARP cache size.

Syntax	no arp cachesize
Command Mode	Global Config

9.1.3. arp dynamicrenew

This command enables the ARP component to renew automatically dynamic ARP entries when they age out. When an ARP entry reaches its maximum age, the system must decide whether to retain or delete the entry.

If the entry has recently been used to forward data packets, the system will renew the entry by sending an ARP request to the neighbor. If the neighbor responds, the age of the ARP cache entry is reset to 0 without removing the entry from the hardware. Traffic to the host continues to be forwarded in hardware without interruption. If the entry is not being used to forward data packets, then the entry is deleted from the ARP cache, unless the dynamic renew option is enabled. If the dynamic renew option is enabled, the system sends an ARP request to renew the entry. When an entry is not renewed, it is removed from the hardware and subsequent data packets to the host trigger an ARP request. Traffic to the host may be lost until the router receives an ARP reply from the host. Gateway entries, entries for a neighbor router, are always renewed. The dynamic renew option applies only to host entries.

The disadvantage of enabling dynamic renew is that once an ARP cache entry is created, that cache entry continues to take space in the ARP cache as long as the neighbor continues to respond to ARP requests, even if no traffic is being forwarded to the neighbor. In a network where the number of potential neighbors is greater than the ARP cache capacity, enabling dynamic renew could prevent some neighbors from communicating because the ARP cache is full.

Default	disabled
Syntax	arp dynamicrenew
Command Mode	Privileged EXEC

9.1.3.1. no arp dynamicrenew

This command prevents dynamic ARP entries from renewing when they age out.

Syntax	no arp dynamicrenew
Command Mode	Privileged EXEC

9.1.4. arp purge

This command causes the specified IP address to be removed from the ARP cache. Only entries of type dynamic or gateway are affected by this command.

Syntax	arp purge ipaddress
Command Mode	Privileged EXEC

9.1.5. arp resptime

This command configures the ARP request response timeout.

The value for *seconds* is a valid positive integer, which represents the IP ARP entry response timeout time in seconds. The range for *seconds* is between 1-10 seconds.

Default	1
Syntax	arp resptime 1-10
Command Mode	Global Config

9.1.5.1. no arp resptime

This command configures the default ARP request response timeout.

Syntax	no arp resptime
Command Mode	Global Config

9.1.6. arp retries

This command configures the ARP count of maximum request for retries.

The value for *retries* is an integer, which represents the maximum number of request for retries. The range for *retries* is an integer between 0-10 retries.

Default	4
Syntax	arp retries 0-10
Command Mode	Global Config

9.1.6.1. no arp retries

This command configures the default ARP count of maximum request for retries.

Syntax	no arp retries
Command Mode	Global Config

9.1.7. arp timeout

This command configures the ARP entry ageout time.

The value for *seconds* is a valid positive integer, which represents the IP ARP entry ageout time in seconds. The range for *seconds* is between 15-21600 seconds.

Default	1200
Syntax	arp timeout 15-21600
Command Mode	Global Config

9.1.7.1. no arp timeout

This command configures the default ARP entry ageout time.

Syntax	no arp timeout
Command Mode	Global Config

9.1.8. clear arp-cache

This command causes all ARP entries of type dynamic to be removed from the ARP cache. If the gateway keyword is specified, the dynamic entries of type gateway are purged as well.

Syntax	clear arp-cache [gateway]
Command Mode	Privileged EXEC

9.1.9. clear arp-switch

Use this command to clear the contents of the switch entries learned through the Management port. To observe whether this command is successful, *ping* from the remote system to the DUT. Issue the **show arp switch** command to see the ARP entries. Then issue the **clear arp switch** command and check the **show arp switch** entries. There will be no more arp entries.

Syntax	clear arp-switch
Command Mode	Privileged EXEC

9.1.10. show arp

This command displays the Address Resolution Protocol (ARP) cache. The displayed results are not the total ARP entries. To view the total ARP entries, the operator should view the **show arp** results in conjunction with the **show arp switch** results.

Syntax	show arp
Command Mode	Privileged EXEC

Parameter	Definition
Age Time (seconds)	The time it takes for an ARP entry to age out. This is configurable. Age time is measured in seconds.
Response Time (seconds)	The time it takes for an ARP request timeout. This value is configurable. Response time is measured in seconds.
Retries	The maximum number of times an ARP request is retried. This value is configurable.

Parameter	Definition
Cache Size	The maximum number of entries in the ARP table. This value is configurable.
Dynamic Renew Mode	Displays whether the ARP component automatically attempts to renew dynamic ARP entries when they age out.
Total Entry Count Current / Peak	The total entries in the ARP table and the peak entry count in the ARP table.
Static Entry Count Current / Max	The static entry count in the ARP table and maximum static entry count in the ARP table.

The following are displayed for each ARP entry:

Parameter	Definition
IP Address	The IP address of a device on a subnet attached to an existing routing interface.
MAC Address	The hardware MAC address of that device.
Interface	The routing unit/slot/port associated with the device ARP entry.
Type	The type that is configurable. The possible values are Local, Gateway, Dynamic and Static.
Age	The current age of the ARP entry since last refresh (in hh:mm:ss format)

9.1.11. show arp brief

This command displays the brief Address Resolution Protocol (ARP) table information.

Syntax show arp brief

Command Mode Privileged EXEC

Parameter	Definition
Age Time (seconds)	The time it takes for an ARP entry to age out. This value is configurable. Age time is measured in seconds.
Response Time (seconds)	The time it takes for an ARP request timeout. This value is configurable. Response time is measured in seconds.
Retries	The maximum number of times an ARP request is retried. This value is configurable.
Cache Size	The maximum number of entries in the ARP table. This value is configurable.
Dynamic Renew Mode	Displays whether the ARP component automatically attempts to renew dynamic ARP entries when they age out.
Total Entry Count Current / Peak	The total entries in the ARP table and the peak entry count in the ARP table.
Static Entry Count Current / Max	The static entry count in the ARP table and maximum static entry count in the ARP table.

9.1.12. show arp switch

This command displays the contents of the switch.

Syntax show arp switch

Command Mode Privileged EXEC

Parameter	Definition
IP Address	The IP address of a device on a subnet attached to the switch.
MAC Address	The hardware MAC address of that device.
Interface	The routing unit/slot/port associated with the device

9.2. IP Routing Commands

This section describes the commands you use to enable and configure IP routing on the switch.

9.2.1. routing

This command enables IPv4 routing for an interface or range of interfaces. You can view the current value for this function with the show ip brief command. The value is labeled as "Routing Mode".

Default	disabled
Syntax	routing
Command Mode	Interface Config

9.2.1.1. no routing

This command disables routing for an interface.

You can view the current value for this function with the **show ip brief** command. The value is labeled as “Routing Mode”.

Syntax	no routing
Command Mode	Interface Config

9.2.2. ip routing

This command enables the IP Router Admin Mode for the master switch.

Syntax	ip routing
Command Mode	Global Config

9.2.2.1. no ip routing

This command disables the IP Router Admin Mode for the master switch.

Syntax	no ip routing
Command Mode	Global Config

9.2.3. ip address

This command configures an IP address on an interface or range of interfaces. You can also use this command to configure one or more secondary IP addresses on the interface. The command supports RFC 3021 and accepts using 31-bit prefixes on IPv4 point-to-point links. This command adds the label IP address in the command **show ip interface**.

The 31-bit subnet mask is only supported on routing interfaces. The feature is not supported on network port and service port interfaces because ICOS acts as a host, not a router, on these management interfaces.

Syntax	ip address ipaddr {subnetmask |/masklen} [secondary]
Command Mode	Interface Config
<ipaddr>	The IP address of the interface.
<subnetmask>	A 4-digit dotted-decimal number which represents the subnet mask of the interface.
<masklen>	Implements RFC 3021. Using the / notation of the subnet mask, this is an integer that indicates the length of the subnet mask. The range is 5 to 32 bits.

Example: The following example of the command shows the configuration of the subnet mask with an IP address in the dotted decimal format on interface vlan 100.

```
(Routing) (Interface vlan 300)#ip address 192.168.10.1 255.255.255.254
(Routing) (Interface vlan 300)#
```

Example: The next example of the command shows the configuration of the subnet mask with an IP address in the / notation on interface vlan 100.

```
(Routing) (Config)#interface vlan 30
(Routing) (Interface vlan 30)#ip address 192.168.10.1 /31
```

9.2.3.1. no ip address

This command deletes an IP address from an interface. The value for *ipaddr* is the IP address of the interface in a.b.c.d format where the range for a, b, c, and d is 1-255. The value for *subnetmask* is a 4-digit dotted-decimal number which represents the Subnet Mask of the interface. To remove all of the IP addresses (primary and secondary) configured on the interface, enter the command **no ip address**.

Syntax	no ip address [{ipaddr subnetmask [secondary]}]
Command Mode	Interface Config

9.2.4. ip address dhcp

This command enables the DHCPv4 client on an in-band interface so that it can acquire network information, such as the IP address, subnet mask, and default gateway, from a network DHCP server. When DHCP is enabled on the interface, the system automatically deletes all manually configured IPv4 addresses on the interface.

To enable the DHCPv4 client on an in-band interface and send DHCP client messages with the client identifier option (DHCP Option 61), use the **ip address dhcp client-id** configuration command in interface configuration mode.

Default	disabled
Syntax	ip address dhcp [client-id]

Command Mode	Interface Config

Example: In the following example, DHCPv4 is enabled on interface 0/1.

```
(router1) #config
(router1) (Config)#interface 0/1
(router1) (Interface 0/1)#ip address dhcp
```

9.2.4.1. no ip address dhcp

The **no ip address dhcp** releases a leased address and disables DHCPv4 on an interface. The **no** form of the **ip address dhcp client-id** command removes the client-id option and also disables the DHCP client on the in-band interface.

Syntax	no ip addressdhcp [client-id]
Command Mode	Interface Config

9.2.5. ip default-gateway

This command manually configures a default gateway for the switch. Only one default gateway can be configured. If you invoke this command multiple times, each command replaces the previous value.

Syntax	ip default-gateway ipaddr
Command Mode	Global Config

9.2.5.1. no ip default-gateway

This command removes the default gateway address from the configuration.

Syntax	no ip default-gateway ipaddr
Command Mode	Global Config

9.2.6. ip route

This command configures a static route. The *ipaddr* parameter is a valid IP address, and *subnetmask* is a valid subnet mask. The *nexthopip* parameter is a valid IP address of the next hop router. Specifying *Null0* as nexthop parameter adds a static reject route. The optional *preference* parameter is an integer (value from 1 to 255) that allows you to specify the preference value (sometimes called route. Among routes to the same destination, the route with the lowest preference value is the route entered into the forwarding database. By specifying the preference of a static route, you control whether a static route is more or less preferred than routes from dynamic routing protocols. The preference also controls whether a static route is more or less preferred than other static routes to the same destination. A route with a preference of 255 cannot be used to forward traffic.

For the static routes to be visible, you must perform the following steps:

- Enable ip routing globally.
- Enable ip routing for the interface.
- Confirm that the associated link is also up.

Default	preference 1
Syntax	ip route ipaddr subnetmask { nexthopip | Null0 } [preference]
Command Mode	Global Config

9.2.6.1. no ip route

This command deletes a single next hop to a destination static route. If you use the *nexthopip* parameter, the next hop is deleted. If you use the *preference* value, the preference value of the static route is reset to its default.

Syntax	no ip route ipaddr subnetmask [{nexthopip [preference] |Null0}]
Command Mode	Global Config

9.2.7. ip route default

This command configures the default route. The value for nexthopip is a valid IP address of the next hop router. The *preference* is an integer value from 1 to 255. A route with a preference of 255 cannot be used to forward traffic.

Default	preference - 1
Syntax	ip route default nexthopip [preference]
Command Mode	Global Config

9.2.7.1. no ip route default

This command deletes all configured default routes. If the optional *nexthopip* parameter is designated, the specific next hop is deleted from the configured default route, and if the optional preference value is designated, the preference of the configured default route is reset to its default.

Syntax	no ip route default [{nexthopip | preference}]
Command Mode	Global Config

9.2.8. ip route distance

This command sets the default distance (preference) for static routes. Lower route distance values are preferred when determining the best route. The **ip route** and **ip route default** commands allow you to optionally set the distance (preference) of an individual static route. The default distance is used when no distance is specified in these commands. Changing the default distance does not update the distance of existing static routes, even if they were assigned the original default distance. The new default distance will only be applied to static routes created after invoking the **ip route distance** command.

Default	1
Syntax	ip route distance 1-255
Command Mode	Global Config

9.2.8.1. no ip route distance

This command sets the default static route preference value in the router. Lower route preference values are preferred when determining the best route.

Syntax	no ip route distance
Command Mode	Global Config

9.2.9. ip netdirbcast

This command enables the forwarding of network-directed broadcasts on an interface or range of interfaces. When enabled, network directed broadcasts are forwarded. When disabled they are dropped.

Default	disabled
Syntax	ip netdirbcast
Command Mode	Interface Config

9.2.9.1. no ip netdirbcast

This command disables the forwarding of network-directed broadcasts. When disabled, network directed broadcasts are dropped.

Syntax	no ip netdirbcast
Command Mode	Interface Config

9.2.10. ip mtu

This command sets the IP Maximum Transmission Unit (MTU) on a routing interface or range of interfaces. The IP MTU is the size of the largest IP packet that can be transmitted on the interface without fragmentation. Forwarded packets are dropped if they exceed the IP MTU of the outgoing interface.

Packets originated on the router, such as OSPF packets, may be fragmented by the IP stack.

OSPF advertises the IP MTU in the Database Description packets it sends to its neighbors during database exchange. If two OSPF neighbors advertise different IP MTUs, they will not form an adjacency (unless OSPF has been instructed to ignore differences in IP MTU with the **ip ospf mtu-ignore** command).

The IP MTU size refers to the maximum size of the IP packet (IP Header + IP payload). It does not include any extra bytes that may be required for Layer-2

headers. To receive and process packets, the Ethernet MTU must take into account the size of the Ethernet header.

Default	1500 bytes
Syntax	ip mtu 68-9198
Command Mode	Interface Config

9.2.10.1. no ip mtu

This command resets the ip mtu to the default value.

Syntax	no ip mtu
Command Mode	Interface Config

9.2.11. encapsulation

This command configures the link layer encapsulation type for the packet on an interface or range of interfaces. The encapsulation type can be ethernet or snap.

Default	ethernet
Syntax	encapsulation {ethernet | snap}
Command Mode	Interface Config

Routed frames are always ethernet encapsulated when a frame is routed to a VLAN.

9.2.12. show dhcp lease

This command displays a list of IPv4 addresses currently leased from a DHCP server on a specific in-band interface or all in-band interfaces. This command does not apply to service or network ports.

Syntax	show dhcp lease [interface {unit/slot/port | vlan id}]
Command Mode	Privileged EXEC

Parameter	Definition
IP address, Subnet mask	The IP address and network mask leased from the DHCP server
DHCP Lease server	The IPv4 address of the DHCP server that leased the address.
State	State of the DHCPv4 Client on this interface
DHCP transaction ID	The transaction ID of the DHCPv4 Client
Lease	The time (in seconds) that the IP address was leased by the server

Parameter	Definition
Renewal	The time (in seconds) when the next DHCP renew Request is sent by DHCPv4 Client to renew the leased IP address
Rebind	The time (in seconds) when the DHCP Rebind process starts
Retry count	Number of times the DHCPv4 client sends a DHCP REQUEST message before the server responds

9.2.13. show ip brief

This command displays the summary information of the IP global configurations for the specified virtual router, including the ICMP rate limit configuration and the global ICMP Redirect configuration. If no router is specified, information related to the default router is displayed.

Syntax show ip brief

Command Mode Privileged EXEC / User EXEC

Parameter	Definition
Default Time to Live	The computed TTL (Time to Live) of forwarding a packet from the local router to the final destination.
Routing Mode	Shows whether the routing mode is enabled or disabled.
Maximum Next Hops	The maximum number of next hops the packet can travel.
Maximum Routes	The maximum number of routes the packet can travel.
ICMP Rate Limit Interval	Shows how often the token bucket is initialized with burst-size tokens. Burst-interval is from 0 to 2147483647 milliseconds. The default burst-interval is 1000 msec.
ICMP Rate Limit Burst Size	Shows the number of ICMPv4 error messages that can be sent during one burst-interval. The range is from 1 to 200 messages. The default value is 100 messages.
ICMP Echo Replies	Shows whether ICMP Echo Replies are enabled or disabled.
ICMP Redirects	Shows whether ICMP Redirects are enabled or disabled.

Example: The following shows example CLI display output for the command.

```
(Routing) #show ip brief
Default Time to Live.......................... 64
Routing Mode.................................. Disabled
Maximum Next Hops............................. 4
Maximum Routes................................ 6000
ICMP Rate Limit Interval...................... 1000 msec
ICMP Rate Limit Burst Size.................... 100 messages
ICMP Echo Replies............................. Enabled
ICMP Redirects................................ Enabled
```

9.2.14. show ip interface

This command displays all pertinent information about the IP interface.

Syntax show ip interface {unit/slot/port | vlan vlan-id}

Command Mode Privileged EXEC / User EXEC

Parameter	Definition
Routing Interface Status	Determine the operational status of IPv4 routing Interface. The possible values are Up or Down.
Primary IP Address	The primary IP address and subnet masks for the interface. This value appears only if you configure it.
Method	Shows whether the IP address was configured manually or acquired from a DHCP server.
Secondary IP Address	One or more secondary IP addresses and subnet masks for the interface. This value appears only if you configure it.
Helper IP Address	The helper IP addresses configured by the command
Routing Mode	The administrative mode of router interface participation. The possible values are enable or disable. This value is configurable.
Administrative Mode	The administrative mode of the specified interface. The possible values of this field are enable or disable. This value is configurable.
Forward Net Directed Broadcasts	Displays whether forwarding of network-directed broadcasts is enabled or disabled. This value is configurable.
Active State	Displays whether the interface is active or inactive. An interface is considered active if its link is up and it is in the forwarding state.
Link Speed Data Rate	An integer representing the physical link data rate of the specified interface. This is measured in Megabits per second (Mbps).
MAC Address	The burned in physical address of the specified interface. The format is 6 two-digit hexadecimal numbers that are separated by colons.
IP MTU	The maximum transmission unit (MTU) size of a frame, in bytes.
Bandwidth	Shows the bandwidth of the interface.
Destination Unreachables	Displays whether ICMP Destination Unreachables may be sent (enabled or disabled).
ICMP Redirects	Displays whether ICMP Redirects may be sent (enabled or disabled).
DHCP Client Identifier	The client identifier is displayed in the output of the command only if DHCP is enabled with the client-id option on the in-band interface.

Example: The following shows example CLI display output for the command.

```
(Routing) #show ip interface 0/2
Routing Interface Status..................... Down
Primary IP Address........................... 1.2.3.4/255.255.255.0
Method....................................... Manual
Secondary IP Address(es)..................... 21.2.3.4/255.255.255.0
.............................................. 22.2.3.4/255.255.255.0
Helper IP Address............................ 1.2.3.4
.............................................. 1.2.3.5
```

```
Routing Mode..................................... Disable
Administrative Mode.............................. Enable
Forward Net Directed Broadcasts.................. Disable
Active State..................................... Inactive
Link Speed Data Rate............................. Inactive
MAC Address...................................... 00:10:18:82:0C:68
Encapsulation Type............................... Ethernet
IP MTU........................................... 1500
Bandwidth........................................ 100000 kbps
Destination Unreachables......................... Enabled
ICMP Redirects................................... Enabled
```

Example: In the following example the DHCP client is enabled on a VLAN routing interface.

```
(Routing) #show ip interface vlan 10
Routing Interface Status.................. Up
Method.................................... DHCP
Routing Mode.............................. Enable
Administrative Mode....................... Enable
Forward Net Directed Broadcasts.......... Disable
Active State.............................. Inactive
Link Speed Data Rate...................... 10 Half
MAC address............................... 00:10:18:82:16:0E
Encapsulation Type........................ Ethernet
IP MTU.................................... 1500
Bandwidth................................. 10000 kbps
Destination Unreachables.................. Enabled
ICMP Redirects............................ Enabled
Interface Suppress Status................. Unsuppressed
DHCP Client Identifier.................... 0icos-0010.1882.160E-vl10
```

9.2.15. show ip interface brief

This command displays summary information about IP configuration settings for all ports in the router, and indicates how each IP address was assigned for a specified virtual router instance. If a virtual router is not specified, the IP configuration settings cache for the default router is displayed.

Syntax	show ip interface brief
Command Mode	Privileged EXEC / User EXEC

Parameter	Definition
Interface	Valid slot and port number separated by a forward slash.
State	Routing operational state of the interface.
IP Address	The IP address of the routing interface in 32-bit dotted decimal format.
IP Mask	The IP mask of the routing interface in 32-bit dotted decimal format.
Method	Indicates how each IP address was assigned. The field contains one of the following values: • DHCP - The address is leased from a DHCP server.

Parameter	Definition
	• Manual - The address is manually configured.

Example: The following shows example CLI display output for the command.

```
(alpha1) #show ip interface brief
Interface State IP Address IP Mask Method
---------- ----- --------------- --------------- --------
0/17 Up 192.168.75.1 255.255.255.0 DHCP
0/19 Up unnumbered
```

9.2.16. show ip route

This command displays the routing table. The *ip-address* specifies the network for which the route is to be displayed and displays the best matching best-route for the address. The *mask* specifies the subnet mask for the given *ip-address*. When you use the *longer-prefixes* keyword, the *ip-address* and *mask* pair becomes the prefix, and the command displays the routes to the addresses that match that prefix. Use the *protocol* parameter to specify the protocol that installed the routes. The value for the *protocol* can be *ospf*, *bgp*, *connected*, or *static*. Use the *all* parameter to display all routes including best and non-best routes. If you do not use the *all* parameter, the command only displays the best route.

If you use the *connected* keyword for the *protocol*, the *all* option is not available because there are no best or non-best connected routes.

Syntax	show ip route [{ip-address [protocol] | {ip-address mask [longer-prefixes] [protocol]}}]
Command Mode	Privileged EXEC / User EXEC

Parameter	Definition
Route Codes	The key for the routing protocol codes that might appear in the routing table output.

The **show ip route** command displays the routing tables in the following format:

Code IP-Address/Mask [Preference/Metric] via Next-Hop, Route-Timestamp, Interface, Truncated

The columns for the routing table display the following information:

Parameter	Definition
Code	The codes for the routing protocols that created the routes.
Default Gateway	The IP address of the default gateway. When the system does not have a more specific route to a packet's destination, it sends the packet to the default gateway.
IP-Address/Mask	The IP-Address and mask of the destination network corresponding to this route.
Preference	The administrative distance associated with this route. Routes with low values are preferred over routes with higher values.

Parameter	Definition
Metric	The cost associated with this route.
via Next-Hop	The outgoing router IP address to use when forwarding traffic to the next router (if any) in the path toward the destination.
Route-Timestamp	The last updated time for dynamic routes. The format of Route-Timestamp will be • Days:Hours:Minutes if days >= 1 • Hours:Minures:Seconds if days <1
Interface	The outgoing router interface to use when forwarding traffic to the next destination. For reject routes, the next hop interface would be Null0 interface.
T	A flag appended to a route to indicate that it is an ECMP route, but only one of its next hops has been installed in the forwarding table. The forwarding table may limit the number of ECMP routes or the number of ECMP groups. When an ECMP route cannot be installed because such a limit is reached, the route is installed with a single next hop. Such truncated routes are identified by a **T** after the interface name.

To administratively control the traffic destined to a particular network and prevent it from being forwarded through the router, you can configure a static reject route on the router. Such traffic would be discarded, and the ICMP destination unreachable message is sent back to the source. This is typically used for preventing routing loops. The reject route added in the RTO is of the type **OSPF Inter-Area**. Reject routes (routes of REJECT type installed by any protocol) are not redistributed by OSPF. Reject routes are supported in OSPFv2.

Example: The following shows example CLI display output for the command.

```
(Routing) #show ip route
Route Codes: O - OSPF Derived, C - Connected, S - Static
B - BGP Derived, IA - OSPF Inter Area
E1 - OSPF External Type 1, E2 - OSPF External Type 2
N1 - OSPF NSSA External Type 1, N2 - OSPF NSSA External Type 2,S
Default gateway is 1.1.1.2
```

```
C 1.1.1.0/24 [0/1] directly connected,
0/11 C 2.2.2.0/24 [0/1] directly connected,
0/1 C 5.5.5.0/24 [0/1] directly connected,
0/5 S 7.0.0.0/8 [1/0] directly connected, Null0
OIA 10.10.10.0/24 [110/6] via 5.5.5.2,   00h:00m:01s,
0/5 C 11.11.11.0/24 [0/1] directly connected,
0/11 S 12.0.0.0/8 [5/0] directly connected, Null0
S 23.0.0.0/8 [3/0] directly connected, Null0
```

Example: The following shows example CLI display output for the command to indicate a truncated route.

```
(router) #show ip route
Route Codes: R - RIP Derived, O - OSPF Derived, C - Connected, S - Static
B - BGP Derived, IA - OSPF Inter Area
```

```
E1 - OSPF External Type 1, E2 - OSPF External Type 2
N1 - OSPF NSSA External Type 1, N2 - OSPF NSSA External Type 2

O E1   100.1.161.0/24 [110/10] via 172.20.11.100,   00h:00m:13s,  2/11 T
O E1   100.1.162.0/24 [110/10] via 172.20.11.100,   00h:00m:13s,  2/11 T
O E1   100.1.163.0/24 [110/10] via 172.20.11.100,   00h:00m:13s,  2/11 T
```

9.2.17. show ip route summary

Use this command to display the routing table summary. When the optional all keyword is given, some statistics, such as the number of routes from each source, include counts for alternate routes. An alternate route is a route that is not the most preferred route to its destination and, therefore, is not installed in the forwarding table. To include only the number of best routes, do not use the optional keyword.

Syntax	show ip route summary [all]
Command Mode	Privileged EXEC / User EXEC

Parameter	Definition
Connected Routes	The total number of connected routes in the routing table.
Static Routes	Total number of static routes in the routing table.
RIP Routes	Total number of routes installed by RIP protocol.
BGP Routes	Total number of routes installed by BGP protocol.
External	The number of external BGP routes.
Internal	The number of internal BGP routes.
Local	The number of local BGP routes.
OSPF Routes	Total number of routes installed by OSPF protocol.
Intra Area Routes	Total number of Intra Area routes installed by OSPF protocol.
Inter Area Routes	Total number of Inter Area routes installed by OSPF protocol.
External Type-1 Routes	Total number of External Type-1 routes installed by OSPF protocol.
External Type-2 Routes	Total number of External Type-2 routes installed by OSPF protocol.
Reject Routes	Total number of reject routes installed by all protocols.
Net Prototype Routes	The number of net-prototype routes.
Total Routes	Total number of routes in the routing table.
Best Routes (High)	The number of best routes currently in the routing table. This number only counts the best route to each destination.
Alternate Routes	The number of alternate routes currently in the routing table. An alternate route is a route that was not selected as the best route to its destination.
Route Adds	The number of routes that have been added to the routing table.

Parameter	Definition
Route Modifies	The number of routes that have been changed after they were initially added to the routing table.
Route Deletes	The number of routes that have been deleted from the routing table.
Unresolved Route Adds	The number of routes adds that failed because none of the router subnet. Note that static routes can fail to be added to the routing table at startup because the routing interfaces are not yet up. This counter gets incremented in this case. The static routes are added to the routing table when the routing interfaces come up.
Invalid Route Adds	The number of routes that failed to be added to the routing table because the route was invalid. A log message is written for each of these failures.
Failed Route Adds	The number of routes that failed to be added to the routing table because of a resource limitation in the routing table.
Reserved Locals	The number of routing table entries reserved for a local subnet on a routing interface that is down. Space for local routes is always reserved so that local routes can be installed when a routing interface bounces.
Unique Next Hops	The number of distinct next hops used among all routes currently in the routing table. These include local interfaces for local routes and neighbors for indirect routes.
Unique Next Hops High Water	The highest count of unique next hops since counters were last cleared.
Next Hop Groups	The current number of next hop groups in use by one or more routes. Each next hop group includes one or more next hops.
Next Hop Groups High Water	The highest count of next hop groups since counters were last cleared.
ECMP Groups (High)	The number of next hop groups with multiple next hops. The value in parentheses indicates the highest count of next hop groups since counters were last cleared.
ECMP Groups	The number of next hop groups with multiple next hops.
ECMP Routes	The number of routes with multiple next hops currently in the routing table.
Truncated ECMP Routes	The number of ECMP routes that are currently installed in the forwarding table with just one next hop. The forwarding table may limit the number of ECMP routes or the number of ECMP groups. When an ECMP route cannot be installed because such a limit is reached, the route is installed with a single next hop.
ECMP Retries	The number of ECMP routes that have been installed in the forwarding table after initially being installed with a single next hop.
Routes with n Next Hops	The current number of routes with each number of next hops.

Example: The following shows example CLI display output for the command.

```
(Routing) #show ip route summary
```

```
Connected Routes.............................. 7
Static Routes................................. 1
OSPF Routes................................... 1004
Intra Area Routes............................. 4
Inter Area Routes............................. 1000
External Type-1 Routes........................ 0
External Type-2 Routes........................ 0
Reject Routes................................. 0
Total routes.................................. 1032
Best Routes (High)............................ 1032 (1032)
Alternate Routes.............................. 0
Route Adds.................................... 1010
Route Modifies................................ 1
Route Deletes................................. 10
Unresolved Route Adds......................... 0
Invalid Route Adds............................ 0
Failed Route Adds............................. 0
Reserved Locals............................... 0
Unique Next Hops (High)....................... 13 (13)
Next Hop Groups (High)........................ 13 (14)
ECMP Groups (High)............................ 2 (3)
ECMP Routes................................... 1001
Truncated ECMP Routes......................... 0
ECMP Retries.................................. 0
Routes with 1 Next Hop........................ 31
Routes with 2 Next Hops....................... 1
Routes with 4 Next Hops....................... 1000
```

9.2.18. clear ip route counters

The command resets to zero the IPv4 routing table counters reported in the command Section 9.2.17, “show ip route summary” for the specified virtual router. If no router is specified, the command is executed for the default router. The command only resets event counters. Counters that report the current state of the routing table, such as the number of routes of each type, are not reset.

Syntax	clear ip route counters
Command Mode	Privileged EXEC

9.2.19. show ip route preferences

This command displays detailed information about the route preferences for each type of route. Route preferences are used in determining the best route. Lower router preference values are preferred over higher router preference values. A route with a preference of 255 cannot be used to forward traffic.

Syntax	show ip route preferences
Command Mode	Privileged EXEC / User EXEC

Parameter	Definition
Local	The local route preference value.
Static	The static route preference value.
BGP External	The BGP external route preference value.
OSPF Intra	The OSPF Intra route preference value.
OSPF Inter	The OSPF Inter route preference value.
OSPF External	The OSPF External route preference value.
RIP	The RIP route preference value.
Internal BGP	The BGP internal route preference value.
Local BGP	The BGP local route preference value.
Configured Default Gateway	The route preference value of the statically-configured default gateway
DHCP Default Gateway	The route preference value of the default gateway learned from the DHCP server.

Example: The following shows example CLI display output for the command.

```
(alpha-stack) #show ip route preferences
Local. ..................................... 0
Static. .................................... 1
BGP External. .............................. 20
OSPF Intra. ................................ 110
OSPF Inter. ................................ 110
OSPF External. ............................. 110
RIP. ....................................... 120
BGP Internal. ..............................200
BGP Local ..................................200
Configured Default Gateway. ................253
DHCP Default Gateway .......................254
```

9.2.20. show ip stats

This command displays IP statistical information. Refer to RFC 1213 for more information about the fields that are displayed.

Syntax	show ip stats
Command Mode	Privileged EXEC / User EXEC

9.2.21. show routing heap summary

This command displays a summary of the memory allocation from the routing heap. The routing heap is a chunk of memory set aside when the system boots for use by the routing applications.

Syntax	show routing heap summary

Command Mode Privileged EXEC

Parameter	Definition
Heap Size	The amount of memory, in bytes, allocated at startup for the routing heap.
Memory In Use	The number of bytes currently allocated.
Memory on Free List	The number of bytes currently on the free list. When a chunk of memory from the routing heap is freed, it is placed on a free list for future reuse.
Memory Available in Heap	The number of bytes in the original heap that have never been allocated.
In Use High Water Mark	The maximum memory in use since the system last rebooted.

Example: The following shows example CLI display output for the command.

```
(Router) #show routing heap summary
Heap Size ..................................... 95053184
Memory In Use ................................. 56998
Memory on Free List ........................... 47
Memory Available in Heap ...................... 94996170
In Use High Water Mark ........................ 57045
```

Chapter 10. Quality of Service Commands

The QoS Commands chapter contains the following sections:

10.1. 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.

Commands you issue in the Interface Config mode only affect a single interface. Commands you issue in the Global Config mode affect all interfaces.

10.1.1. 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 0-6, although the actual number of available traffic classes depends on the platform.

Syntax	classofservice dot1p-mapping userpriority trafficclass
Command Mode	Global Config / Interface Config

10.1.1.1. no classofservice dot1p-mapping

This command maps each 802.1p priority to its default internal traffic class value.

Syntax	no classofservice dot1p-mapping
Command Mode	Global Config / Interface Config

10.1.2. classofservice ip-dscp-mapping

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

The *trafficclass* values can range from 0-6, although the actual number of available traffic classes depends on the platform.

Syntax	classofservice ip-dscp-mapping ipdscp trafficclass
Command Mode	Global Config

10.1.2.1. no classofservice ip-dscp-mapping

This command maps each IP DSCP value to its default internal traffic class value.

Syntax	no classofservice ip-dscp-mapping
Command Mode	Global Config

10.1.3. 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. 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 command because Dot1p is the default.

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
Syntax	classofservice trust {dot1p | ip-dscp | untrusted}
Command Mode	Global Config / Interface Config

10.1.3.1. no classofservice trust

This command sets the interface mode to the default value.

Syntax	no classofservice trust
Command Mode	Global Config / Interface Config

10.1.4. 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. The total number of queues supported per interface is platform specific. 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.

Syntax	cos-queue min-bandwidth bw-0 bw-1 … bw-n
Command Mode	Global Config / Interface Config

10.1.4.1. no cos-queue min-bandwidth

This command restores the default for each queue’s minimum bandwidth value.

Syntax	no cos-queue min-bandwidth
Command Mode	Global Config / Interface Config

10.1.5. 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.

Syntax	cos-queue random-detect queue-id-1 [queue-id-2 … queue-id-n]
Command Mode	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 support per interface. The number *n* is platform dependent and corresponds to the number of supported queues (traffic classes).

10.1.5.1. 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.

Syntax	no cos-queue random-detect queue-id-1 [queue-id-2 … queue-id-n]
Command Mode	Global Config / Interface Config

10.1.6. 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.

Syntax	cos-queue strict queue-id-1 [queue-id-2 … queue-id-n]
Command Mode	Global Config / Interface Config

10.1.6.1. no cos-queue strict

This command restores the default weighted scheduler mode for each specified queue.

Syntax	no cos-queue strict queue-id-1 [queue-id-2 … queue-id-n]
Command Mode	Global Config / Interface Config

10.1.7. 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.

Syntax	random-detect

Command Mode	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. The Interface Config mode command is only available on platforms that support independent per-port class of service queue configuration.

10.1.7.1. no random-detect

Use this command to disable WRED, thereby restoring the default tail drop operation for all queues on the interface.

Syntax	no random-detect
Command Mode	Global Config / Interface Config

10.1.8. random-detect exponential weighting-constant

This command is used to configure the WRED decay exponent for a CoS queue interface.

Syntax	random-detect exponential-weighting-constant 1-TBD
Command Mode	Global Config / Interface Config

10.1.8.1. no random-detect exponential-weighting-constant

Use this command to set the WRED decay exponent back to the default.

Syntax	no random-detect exponential-weighting-constant
Command Mode	Global Config / Interface Config

10.1.9. 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).

Syntax	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
Command Mode	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.

<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).

10.1.9.1. no random-detect queue-parms

Use this command to set the WRED configuration back to the default.

Syntax	no random-detect queue-parms queue-id-1 [queue-id-2 … queue-id-n]
Command Mode	Global Config / Interface Config

10.1.10. traffic-shape

This command specifies the maximum transmission bandwidth limit for the interface as a whole. 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.

Syntax	traffic-shape bw
Command Mode	Global Config / Interface Config

10.1.10.1. no traffic-shape

This command restores the interface shaping rate to the default value.

Syntax	no traffic-shape
Command Mode	Global Config / Interface Config

10.1.11. show classofservice dot1p-mapping

This command displays the current display Dot1p (802.1p) priority mapping to internal traffic classes for a specific interface. The *unit/slot/port* parameter is optional and is only valid on platforms that support independent per-port class of service mappings. If specified, the 802.1p mapping table of the interface is displayed. If omitted, the most recent global configuration settings are displayed.

Syntax	show classofservice dot1p-mapping [unit/slot/port]
Command Mode	Privileged EXEC

The following information is repeated for each user priority.

Parameter	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.

10.1.12. show classofservice ip-precedence-mapping

This command displays the current IP Precedence mapping to internal traffic classes for a specific interface. The *unit/slot/port* parameter is optional and is only valid on platforms that support independent per-port class of service mappings. If specified, the IP Precedence mapping table of the interface is displayed. If omitted, the most recent global configuration settings are displayed.

Syntax	show classofservice ip-precedence-mapping [unit/slot/port]
Command Mode	Privileged EXEC

The following information is repeated for each user priority.

Parameter	Definition
IP Precedence	The IP Precedence value.
Traffic Class	The traffic class internal queue identifier to which the IP Precedence value is mapped.

10.1.13. show classofservice ip-dscp-mapping

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

Syntax	show classofservice ip-dscp-mapping
Command Mode	Privileged EXEC

The following information is repeated for each user priority.

Parameter	Definition
IP DSCP	The IP DSCP value.
Traffic Class	The traffic class internal queue identifier to which the IP DSCP value is mapped.

10.1.14. show classofservice trust

This command displays the current trust mode setting for a specific interface. The *unit/slot/port* parameter is optional and is only valid on platforms that support independent per-port class of service mappings. 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.

Syntax show classofservice trust [unit/slot/port]

Command Mode Privileged EXEC

Parameter	Definition
Non-IP Traffic Class	The traffic class used for non-IP traffic. This is only displayed when the COS trust mode is set to trust IP Precedence or IP DSCP (on platforms that support IP DSCP)
Untrusted Traffic Class	The traffic class used for all untrusted traffic. This is only displayed when the COS trust mode is set to *untrusted*.

10.1.15. show interfaces cos-queue

This command displays the class-of-service queue configuration for the specified interface. The *unit/slot/port* parameter is settings are displayed.

Syntax show interfaces cos-queue [unit/slot/port]

Command Mode Privileged EXEC

Parameter	Definition
Queue Id	An interface supports n queues numbered 0 to (n-1). The specific n value is platform dependent.
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.

Parameter	Definition
Interface	The unit/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.

10.1.16. show interfaces random-detect

This command displays the global WRED settings for each CoS queue. If you specify the *unit/slot/port*, the command displays the WRED settings for each CoS queue on the specified interface.

Syntax show interfaces random-detect [unit/slot/port]

Command Mode Privileged EXEC

Parameter	Definition
Queue ID WRED Minimum	An interface supports n queues numbered 0 to (n-1). The n value is platform dependent.
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).

10.2. 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:

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 recreate it.

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.

10.2.1. 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.

Syntax	diffserv
Command Mode	Global Config

10.2.1.1. 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.

Syntax	no diffserv
Command Mode	Global Config

10.3. 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.

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 recreate the entire class.

The CLI command root is *class-map*.

10.3.1. 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.

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.

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.

The optional keyword appiq creates a new DiffServ appiq class. Regular expressions found in the traffic patterns in layer 7 applications can be matched to the App-IQ class using a match signature command.

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.

Syntax	class-map match-all class-map-name [{appiq | ipv4 | ipv6}]
Command Mode	Global Config

10.3.1.1. 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.

Syntax	no class-map class-map-name
Command Mode	Global Config

10.3.2. 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
Syntax	class-map rename class-map-name new-class-map-name
Command Mode	Global Config

10.3.3. 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, 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.

Syntax	match [not] ethertype {keyword | custom 0x0600-0xFFFF}
Command Mode	Class-Map Config

10.3.4. 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
Syntax	match [not] any
Command Mode	Class-Map Config

10.3.5. 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
Syntax	match class-map refclassname
Command Mode	Class-Map Config

NOTE:

- 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 allowed combination based on the class type.
- Any subsequent changes to the refclassname class match criteria must maintain this validity, or the changes 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.

10.3.5.1. 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.

Syntax	no match class-map refclassname
Command Mode	Class-Map Config

10.3.6. 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.

Default	none
Syntax	match cos 0-7
Command Mode	Class-Map Config

10.3.7. 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.

This command is supported on the following platforms: BCM56314, BCM56504, BCM56214, BCM56224

Default	none
Syntax	match [not] secondary-cos 0-7
Command Mode	Class-Map Config

10.3.8. 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
Syntax	match [not] destination-address mac macaddr macmask
Command Mode	Class-Map Config

10.3.9. 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
Syntax	match [not] dstip ipaddr ipmask
Command Mode	Class-Map Config

10.3.10. match dstip6

This command adds to the specified class definition a match condition based on the destination IPv6 address of a packet. Use the [not] option to negate the match condition.

Default	none

Syntax	match [not] dstip6 destination-ipv6-prefix/prefix-length
Command Mode	Ipv6-Class-Map Config

10.3.11. 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, 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
Syntax	match [not] dstl4port {portkey | 0-65535}
Command Mode	Class-Map Config

10.3.12. 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 dscpvalvalue 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.

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
Syntax	match ip dscp dscpval
Command Mode	Class-Map Config

10.3.13. 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.

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
Syntax	match [not] ip precedence 0-7
Command Mode	Class-Map Config

10.3.14. 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.

The IP DSCP, IP Precedence, and I 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.

This complete control when specifying which bits of the IP Service Type field are checked.

Default	none
Syntax	match [not] ip tos tosbits tosmask
Command Mode	Class-Map Config

10.3.15. match ip6flowlbl

Use this command to enter an IPv6 flow label value. Use the [not] option to negate the match condition.

Default	none
Syntax	match [not] ip6flowlbl label 0-1048575
Command Mode	Ipv6-Class-Map Config

10.3.16. 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.

This command does not validate the protocol number value against the current list defined by IANA.

Default	none
Syntax	match [not] protocol {protocol-name | 0-255}
Command Mode	Class-Map Config

10.3.17. 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
Syntax	match [not] source-address mac address macmask
Command Mode	Class-Map Config

10.3.18. 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
Syntax	match [not] srcip ipaddr ipmask
Command Mode	Class-Map Config

10.3.19. match srcip6

This command adds to the specified class definition a match condition based on the source IP address of a packet. Use the [not] option to negate the match condition.

Default	none
Syntax	match [not] srcip6 source-ipv6-prefix/prefix-length

Command Mode	Ipv6-Class-Map Config

10.3.20. 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, 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
Syntax	match not srcl4port {portkey | 0-65535}
Command Mode	Class-Map Config

10.3.21. match src port

This command adds a match condition for a range of layer source 4 ports. If an interface receives traffic that is within the configured range of layer 4 source ports, then only the *appiq* class is in effect. *portvalue* specifies a single source port.

Default	none
Syntax	match src port {portstart-portend | portvalue}
Command Mode	Class-Map Config

10.3.22. 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 4095. Use the [not] option to negate the match condition.

Default	none
Syntax	match [not] vlan 0-4095
Command Mode	Class-Map Config

10.3.23. 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 4095. Use the [not] option to negate the match condition.

Default	none
Syntax	match [not] secondary-vlan 0-4095
Command Mode	Class-Map Config

10.4. 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.

The only way to remove an individual policy attribute from a class instance within a policy is to remove the class instance and readd 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*.

10.4.1. 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.

Syntax	assign-queue queueid
Command Mode	Policy-Class-Map Config
Incompatibilities	Drop

10.4.2. drop

This command specifies that all packets for the associated traffic stream are to be dropped at ingress.

Syntax	drop
Command Mode	Policy-Class-Map Config
Incompatibilities	Assign Queue, Mark (all forms), Mirror, Police, Redirect

10.4.3. mirror

This command specifies that all incoming packets for the associated traffic stream are copied to a specific egress interface (physical port or LAG).

Syntax	mirror unit/slot/port
Command Mode	Policy-Class-Map Config
Incompatibilities	Drop, Redirect

10.4.4. 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).

Syntax	redirectunit/slot/port
Command Mode	Policy-Class-Map Config
Incompatibilities	Drop, Mirror

10.4.5. 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.

This command may only be used after specifying a police command for the policy-class instance.

Syntax	conform-color class-map-name
Command Mode	Policy-Class-Map Config

10.4.6. 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.

This command causes the specified policy to create a reference to the class definition.

The CLI mode is changed to Policy-Class-Map Config when this command is successfully executed.

Syntax	class classname
Command Mode	Policy-Class-Map Config

10.4.6.1. 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.

This command removes the reference to the class definition for the specified policy.

Syntax	no class classname
Command Mode	Policy-Class-Map Config

10.4.7. 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
Syntax	mark-cos 0-7
Command Mode	Policy-Class-Map Config
Incompatibilities	Drop, Mark IP DSCP, IP Precedence, Police

10.4.8. mark secondary-cos

This command marks all packets for the associated traffic stream with the specified secondary class of service (CoS) value in the priority field of the 802.1p header (the secondary or inner 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.

Syntax	mark secondary-cos 0-7
Command Mode	Policy-Class-Map Config
Incompatibilities	Drop, Mark IP DSCP, IP Precedence, Police

10.4.9. 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.

Syntax	mark-cos-as-sec-cos
Command Mode	Policy-Class-Map Config

Incompatibilities	Drop, Mark IP DSCP, IP Precedence, Police

Example: The following shows an example of the command.

```
(Routing) (Config-policy-classmap)#mark cos-as-sec-cos
```

10.4.10. 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.

Syntax	mark ip-dscp dscpval
Command Mode	Policy-Class-Map Config
Incompatibilities	Drop, Mark CoS, Mark IP Precedence, Police

10.4.11. 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.

Syntax	mark ip-precedence 0-7
Command Mode	Policy-Class-Map Config
Incompatibilities	Drop, Mark CoS, Mark IP Precedence, Police Policy Type In

10.4.12. 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.

Syntax	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}]}
Command Mode	Policy-Class-Map Config
Incompatibilities	Drop, Mark (all forms)

Example: The following shows an example of the command.

```
(Routing) (Config-policy-classmap)#police-simple 1 128 conform-action
transmit violate-action drop
```

10.4.13. 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.

Syntax	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-transmit0-7 | set-sec-cos-transmit 0-7 | set-prec-transmit 0-7 | set- dscp-transmit 0-63 | transmit}]}
Command Mode	Policy-Class-Map Config

10.4.14. 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.

Syntax	police-two-rate {1-42949672951-42949672951-1281-128 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-transmit0-7 | 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}]}
Command Mode	Policy-Class-Map Config

10.4.15. 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.

The CLI mode is changed to Policy-Map Config when this command is successfully executed.

Syntax	policy-map policyname in
Command Mode	Global Config

10.4.15.1. 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.

Syntax	no policy-map policyname
Command Mode	Global Config

10.4.16. policy-map rename

This command changes the name of a DiffServ policy. The *policyname* is 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.

Syntax	policy-map rename policyname newpolicyname
Command Mode	Global Config

10.5. 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*.

10.5.1. service-policy

This command attaches a policy to an interface in the inbound direction. The *policyname* parameter is the name of an existing DiffServ policy. This command causes a service to create a reference to the policy.

This command effectively enables DiffServ on an interface in the inbound direction. There is no separate interface administrative *mode* command for DiffServ.

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.

Syntax	service-policy in policymapname
Command Mode	Golbal Config / Interface Config

Each interface can have one policy attached

10.5.1.1. no service-policy

This command detaches a policy from an interface in the inbound direction. The *policyname* parameter is the name of an existing DiffServ policy.

This command causes a service to remove its reference to the policy. This command effectively disables DiffServ on an interface in the inbound direction. There is no separate interface administrative *mode* command for DiffServ.

Syntax	no service-policy in policymapname
Command Mode	Golbal Config / Interface Config

10.6. 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.

10.6.1. show class-map

This command displays all configuration information for the specified class. The *class-name* is the name of an existing DiffServ class.

Syntax	show class-map class-name
Command Mode	Privileged EXEC / User EXEC

If the class-name is specified the following fields are displayed:

Parameter	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.
L3 Proto	The Layer 3 protocol for this class. Possible value is IPv4.
Match Criteria	The Match Criteria fields are only displayed if they have been configured. Not all platforms support all match criteria values. They 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:

Parameter	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.

10.6.2. 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.

Syntax show diffserv

Command Mode Privileged EXEC

Parameter	Definition
DiffServ Admin mode	The current value of the DiffServ administrative mode.
Class Table Size	The current number of entries (rows) in the Class Table.
Class Table Max	The maximum allowed entries (rows) for the Class Table.
Class Rule Table Size	The current number of entries (rows) in the Class Rule Table.
Class Rule Table Max	The maximum allowed entries (rows) for the Class Rule Table.
Policy Table Size	The current number of entries (rows) in the Policy Table.
Policy Table Max	The maximum allowed entries (rows) for the Policy Table.
Policy Instance Table Size	Current number of entries (rows) in the Policy Instance Table.
Policy Instance Table Max	Maximum allowed entries (rows) for the Policy Instance Table.
Policy Attribute Table Size	Current number of entries (rows) in the Policy Attribute Table.
Policy Attribute Table Max	Maximum allowed entries (rows) for the Policy Attribute Table.
Service Table Size	The current number of entries (rows) in the Service Table.
Service Table Max	The maximum allowed entries (rows) for the Service Table.

10.6.3. show policy-map

This command displays all configuration information for the specified policy. The *policyname* is the name of an existing DiffServ policy.

Syntax show policy-map [policyname]

Command Mode Privileged EXEC

If the Policy Name is specified the following fields are displayed:

Parameter	Definition
Policy Name	The name of this policy.
Policy Type	The policy type (only inbound policy definitions are supported for this platform.)

The following information is repeated for each class associated with this policy (only those policy attributes actually configured are displayed):

Parameter	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.
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.
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/remark 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/remark 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. This field does not display on Broadcom 5630x platforms.

Parameter	Definition
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.
Peak Rate	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 hopit 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).
Class Members	List of all class names associated with this policy.

If the Policy Name is not specified this command displays a list of all defined DiffServ policies. The following fields are displayed:

Parameter	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.

Example: The following shows example CLI display output including the mark-cos-as-sec-cos option specified in the policy action.

```
(Routing) #show policy-map p1
Policy Name..................................... p1
Policy Type..................................... In
Class Name...................................... c1
Mark CoS as Secondary CoS....................... Yes
```

Example: 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.

```
(Routing) #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
```

10.6.4. show diffserv service

This command displays policy service information for the specified interface and direction. The *unit/slot/port* parameter specifies a valid *unit/slot/port* number for the system.

Syntax	show diffserv service unit/slot/port in
Command Mode	Privileged EXEC

Parameter	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	unit/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.
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).

10.6.5. 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.

Syntax	show diffserv service brief [in]
Command Mode	Privileged EXEC
<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):

Parameter	Definition
Interface	unit/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.

10.6.6. show policy-map interface

This command displays policy-oriented statistics information for the specified interface and direction. The *unit/slot/port* parameter specifies a valid interface for the system.

This command is only allowed while the DiffServ administrative mode is enabled.

Syntax	show policy-map interface {unit/slot/port | lag lag-id} [in]
Command Mode	Privileged EXEC
<Interface>	The port or LAG associated with the policy.
<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:

Parameter	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.

10.6.7. show service-policy

This command displays a summary of policy-oriented statistics information for all interfaces in the specified direction.

Syntax	show service-policy [in | out]
Command Mode	Privileged EXEC

The following information is repeated for each interface and direction (only those interfaces configured with an attached policy are shown):

Parameter	Definition
Interface	The interface associated with the service policy.
Operational Status	The current operational status of this DiffServ service interface.
Policy Name	The name of the policy attached to the interface.

10.7. 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 regardless of type. ACL on the same interface.

- 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.
- For the Broadcom 5630x platform, if you configure an IP ACL on an interface, you cannot configure a MAC ACL on the same interface.

10.7.1. 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.

If a MAC ACL by this name already exists, this command enters Mac-Access-List config mode to allow updating the existing MAC ACL.

The CLI mode changes to Mac-Access-List Config mode when you successfully execute this command.

Syntax	mac access-list extended name
Command Mode	Global Config

10.7.1.1. no mac access-list extended

This command deletes a MAC ACL identified by *name* from the system.

Syntax	no mac access-list extended name
Command Mode	Global Config

10.7.2. 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.

Syntax	mac access-list extended rename name newname
Command Mode	Global Config

10.7.3. {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.

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.

An implicit *deny all* MAC rule always terminates the access list.

Only one port can transmit the data flows when enable ACL with rate-limit rule on egress.

For BCM5630x and BCM5650x based systems, assign-queue, redirect, and mirror attributes are configurable for a deny rule, but they have no operational effect.

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.

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, ipx, mplsmcast, mplsucast, netbios, novell, pppoe, rarp. Each of these translates into its equivalent Ethertype value(s).

Table 10.1. Ethertype Keyword and 4-digit Hexadecimal Value

Ethertype Keyword	Corresponding Value
appletalk	0x809B
arp	0x0806
ibmsna	0x80D5
ipv4	0x0800
ipx	0x8037
mplsmcast	0x8848
mplsucast	0x8847

Ethertype Keyword	Corresponding Value
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 atime 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, and then the ACL rule is applied immediately. If a time range with the 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 the specified name becomes inactive.

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.

For the Broadcom 5650x platform, the mirror parameter allows the traffic matching this rule to be copied to the specified *unit/slot/port* while the redirect parameter allows the traffic matching this rule to be forwarded to the specified *unit/slot/port*. The *assign-queue* and *redirect* parameters are only valid for a *permit* rule.

The *redirectExtAgent* optional parameter allows matching flow packets to be sent to external applications running alongside FASTPATH on a control CPU. agent-id is a unique identifier for the external receive client application. agent-id is an integer in the range 1 to 100. The redirectExtAgent action is mutually exclusive with the mirror and redirect parameters.

The *rate-limit* option allows the device to permit only the allowed rate of traffic as per the configured rate in kbps, and burst-size in kbytes.

The *mirror* and *redirect* parameters are not available on the Broadcom 5630x platform.

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

Syntax [sequence-number]{deny|permit} { srcmac | any} { dstmac | any} [ethertypekey | 0x0600-0xFFFF] [vlan {eq 0-4095}] [cos 0-7] [{mirror | redirect} unit/slot/port] [redirectExtAgent agent-id] [rate-limit rate burst- size]

Command Mode Mac-Access-List Config

10.7.3.1. no sequence-number

Use this command to remove the ACL rule with the specified sequence number from the ACL.

Syntax	no sequence-number
Command Mode	MAC-Access-List Config

10.7.4. 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. The *Interface Config* mode command is only available on platforms that support independent per-port class of service queue configuration.

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.

The keyword control-plane is only available in Global Config mode.

The availability of the out option is platform-dependent.

Syntax	mac access-group name {in vlan vlan-id in} [sequence 1-4294967295]
Command Mode	Gobal Config / Interface Config

10.7.4.1. no mac access-group

This command removes a MAC ACL identified by name from the interface in a given direction.

Syntax	no mac access-group name {in vlan vlan-id in}
Command Mode	Gobal Config / Interface Config

10.7.5. 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.

Syntax show mac access-lists [name]

Command Mode Privileged EXEC

Parameter	Definition
Rule Number Action	The ordered rule number identifier defined within the MAC ACL.
Source MAC Address	The source MAC address for this rule.
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.
Assign Queue	The queue identifier to which packets matching this rule are assigned.
Mirror Interface	On Broadcom 5650x platforms, the unit/slot/port to which packets matching this rule are copied.
Redirect Interface	On Broadcom 5650x platforms, the unit/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.
Rule Status	Status (Active/Inactive) of the MAC ACL 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.

10.8. 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 neq/lt/gt/range does not support in egress port

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 ACLs on an Interface, you cannot configure an IP ACL on the same interface.
- 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 the zeros(0's) for the bit position that are not used. In contrast, a wildcard mask has (0's) in a bit position 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 ACL mask indicates the corresponding bit can be ignored.

10.8.1. 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. The table below describes the parameters for the access-list command.

IP Standard ACL:

Syntax	access-list 1-99[rule 1-10] { deny | permit } { every | srcip srcmask } [time-range time-range-name][assign-queue queue-id] [{ mirror | redirect } unit/slot/port] [rate-limit rate burst- size]
Command Mode	Global Config

IP Extended ACL:

Syntax	access-list 100-199 [rule 1-10]{ deny | permit } {every | {{icmp | igmp | ip | tcp | udp | 0–255 } {srcip srcmask[{eq {portkey|0-65535}{dstip dstmask[{eq{portkey | 0-65535}] [precedence precedence | tos tos [tosmask] | dscp dscp] [time-range time-range-name] [assign-queue queue-id] [{mirror | redirect} unit/slot/port] [rate-limit rate burst-size]

Command Mode Global Config

IPv4 extended ACLs have the following limitations for egress ACLs:

- Match on port ranges is not supported.
- The rate-limit command is not supported.

Table 10.2. ACL Command Parameters

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 1-10	Specifies the IP access list rule.
{deny / permit}	Specifies whether the IP ACL rule permits or denies an action.
every	Match every packet.
{icmp / igmp / ip / tcp / udp / 0 - 255}	Specifies the protocol (or well-known port number of the protocol) to filter for an extended IP ACL rule.
srcip srcmask	Specifies a source IP address and source netmask for match condition of the IP ACL rule.
{eq {portkey / 0-65535}}	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: domain, echo, ftp, ftpdata, smtp, snmp, telnet, tftp, and www. Each of these keywords translates into its equivalent port number, which is used as both the start and end of a port range.
dstip dstmask	Specifies a destination IP address and netmask for match condition of the IP ACL rule.
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.
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, then the ACL rule is applied when the time-range with specified name becomes active. The ACL rule is emoved 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	For Broadcom 5650x platforms, specifies the mirror or redirect interface which is the unit/slot/port to which packets matching this rule are copied

Parameter	Description
	or forwarded, respectively. The mirror and redirect parameters are not available on the Broadcom 5630x platform.

10.8.1.1. 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.

Syntax	no access-list accesslistnumber [rule 1-1023]
Command Mode	Global Config

10.8.2. 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.

If an IP ACL by this name already exists, this command enters IPv4-Access_List config mode to allow updating the existing IP ACL.

The CLI mode changes to IPv4-Access-List Config mode when you successfully execute this command.

Syntax	ip access-list name
Command Mode	Global Config

10.8.2.1. no ip access-list

This command deletes the IP ACL identified by name from the system.

Syntax	no ip access-list name
Command Mode	Global Config

10.8.3. 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 *newname* 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.

Syntax	ip access-list rename name newname

Command Mode	Global Config

10.8.4. {deny | permit} (IP ACL)

This command creates a new rule for the current IP access 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.

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.

An implicit *deny all* IP rule always terminates the access list.

For BCM5630x-based systems, the mirrorand redirect parameters are not available.

For BCM5650x-based systems, the mirror parameter allows the traffic matching this rule to be copied to the specified unit/slot/port, while the redirect parameter allows the traffic matching this rule to be forwarded to the specified unit/slot/port . The assign-queue and redirect parameters are only valid for a permit rule.

For IPv4, the following are not supported for egress ACLs:

- A match on port ranges.
- The rate-limit command.

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.

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 Section 10.10, “Time Range Commands for Time-Based ACLs”.

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.

Syntax	[rule <1-10>] {deny | permit} {every | {{icmp | igmp | ip | tcp | udp | 0-255} {srcip srcmask } [{eq {portkey | 0-65535}] dstip dstmask [{eq {portkey | 0-65535}] [precedence precedence | tos tos [tosmask] | dscp dscp]}} [time-range time-range-name] [assign-queue queue-id] [{mirror | redirect} unit/slot/port]
Command Mode	Ipv4-Access-List Config

Parameter	Description
rule 1-10	Specifies the IP access list rule.
{deny / permit}	Specifies whether the IP ACL rule permits or denies an action.
every	Match every packet.
{icmp / igmp / ip / tcp / udp / 0 - 255}	Specifies the protocol (or well-known port number of the protocol) to filter for an extended IP ACL rule.
srcip srcmask	Specifies a source IP address and source netmask for match condition of the IP ACL rule.
{eq {portkey / 0-65535}}	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: domain, echo, ftp, ftpdata, smtp, snmp, telnet, tftp, and www. Each of these keywords translates into its equivalent port number, which is used as both the start and end of a port range.
dstip dstmask	Specifies a destination IP address and netmask for match condition of the IP ACL rule.
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.
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, then the ACL rule is applied when the time-range with specified name becomes active. The ACL rule is emoved 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	For Broadcom 5650x platforms, specifies the mirror or redirect interface which is the unit/slot/port to which packets matching this rule are copied or forwarded, respectively. The mirror and redirect parameters are not available on the Broadcom 5630x platform.

10.8.5. ip access-group

This command either attaches a specific IP ACL identified by *accesslistnumber* 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.The implicit "deny all" is only one and at the end if you attach more than 2 ACL list to the same interface.

The keyword control-plane is only available in Global Config mode.

The out option may or may not be available, depending on the platform.

Default	none
Syntax	ip access-group {accesslistnumber|name} {in|vlan vlan-id in} [sequence 1-4294967295]
Command Mode	Global Config / Interface Config

10.8.5.1. no ip access-group

This command removes a specified IP ACL from an interface.

Default	none
Syntax	no ip access-group {accesslistnumber|name} {{control-plane|in|out}|vlan vlan-id {in|out}}
Command Mode	Global Config / Interface Config

10.8.6. 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.

Syntax	show ip access-lists [accesslistnumber | name]

Command Mode Privileged EXEC

Parameter	Definition
ACL ID/Name	Identifies the configured ACL number or name.
Rules	Identifies the number of rules configured for the ACL
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:

Only the access list fields that you configure are displayed.

Parameter	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.
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.
Assign Queue	The queue identifier to which packets matching this rule are assigned.
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.

Parameter	Definition
Committed Rate	The committed rate defined by the rate-limit attribute.
Committed Burst Size	The committed burst size defined by the rate-limit attribute.
Rule Status	Status (Active/Inactive) of the IP ACL rule.

Example: The following shows example CLI display output for the command.

```
(Routing) #show ip access-lists ip1
ACL Name: ip1
Inbound Interface(s): 1/0/30
Sequence Number: 1
Action..................................... permit
Match All.................................. FALSE
Protocol................................... 1(icmp)
ICMP Type……..3(Destination Unreachable)
Starting Source L4 port… .. 80
Ending Source L4 port… .. 85
Starting Destination L4 port… .. 180
Ending Destination L4 port… .. 185
ICMP Code ......... 0
Fragments……. FALSE
Committed Rate. ............................... 32
Committed Burst Size .......................... 16
ACL hit count ..........................0
```

10.8.7. show access-lists

This command displays IP ACLs, IPv6 ACLs, and MAC access control lists information for a designated interface and direction. Use the control-plane keyword to display the ACLs applied on the CPU port.

Syntax	show access-lists interface {{unit/slot/port | lag lag-id} in}
Command Mode	Privileged EXEC

Parameter	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).

Parameter	Definition
in	In - Display access list information for a particular interface and the in direction.

10.8.8. show access-lists vlan

This command displays Access List information for a particular VLAN ID.

Syntax show access-lists vlan vlan-id in

Command Mode Privileged EXEC

Parameter	Definition
vlan-id	A VLAN ID.
in	In - Display access list information for a particular VLAN ID and the in direction.

10.9. 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.

10.9.1. 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.

If an IPv6 ACL by this name already exists, this command enters IPv6-Access-List config mode to allow updating the existing IPv6 ACL.

The CLI mode changes to IPv6-Access-List Config mode when you successfully execute this command.

Syntax	ipv6 access-list name
Command Mode	Global Config

10.9.1.1. no ipv6 access-list

This command deletes the IPv6 ACL identified by name from the system.

Syntax	no ipv6 access-list name
Command Mode	Global Config

10.9.2. 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.

Syntax	ipv6 access-list rename name newname
Command Mode	Global Config

10.9.3. {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.

Syntax	[rule <1-10>] {deny | permit} {every | {{icmpv6 | ipv6 | tcp | udp | 0-255} [[time-range time-range-name] [assign-queue queue-id] [{mirror | redirect} unit/slot/port] [rate-limit rate burst-size]
Command Mode	IPv6-Access-List Config

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.

An implicit **deny all IPv6** rule always terminates the access list.

Do not support flow-lable in egress and routing in ingress.

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 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.

For the Broadcom 5650x platform, the mirror parameter allows the traffic matching this rule to be copied to the specified *unit/slot/port*, while the redirect parameter allows the traffic matching this rule to be forwarded to the specified *unit/slot/port*. The *assign-queue* and *redirect* parameters are only valid for a permit rule.

The mirror and redirect parameters are not available on the Broadcom 5630x platform.

The **permit** command 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
rule 1-10	Specifies the IP access list rule.
{deny / permit}	Specifies whether the IP ACL rule permits or denies an action.
every	Match every packet.
{icmp / igmp / ip / tcp / udp / 0 - 255}	Specifies the protocol (or well-known port number of the protocol) to filter for an extended IP ACL rule.
srcip srcmask	Specifies a source IP address and source netmask for match condition of the IP ACL rule.
{eq {portkey / 0-65535}}	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: domain, echo, ftp, ftpdata, smtp, snmp, telnet, tftp, and www. Each of these keywords translates into its equivalent port number, which is used as both the start and end of a port range.
dstip dstmask	Specifies a destination IP address and netmask for match condition of the IP ACL rule.
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.
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, then the ACL rule is applied when the time-range with specified name becomes active. The ACL rule is emoved 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	For Broadcom 5650x platforms, specifies the mirror or redirect interface which is the unit/slot/port to which packets matching this rule are copied or forwarded, respectively. The mirror and redirect parameters are not available on the Broadcom 5630x platform.

Example: the following shows an example of the command.

```
(Routing) (Config)#ipv6 access-list ip61
(Routing) (Config-ipv6-acl)#permit udp any any rate-limit 32 16
(Routing) (Config-ipv6-acl)#exit
```

10.9.4. 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 specified IPv6 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. The Interface Config mode command is only available on platforms that support independent per-port class of service queue configuration.

You should be aware that the *out* option may or may not be available, depending on the platform.

Syntax	ipv6 traffic-filter name {in|vlan vlan-id in} [sequence 1-4294967295]
Command Mode	Interface Config

Example: The following shows an example of the command.

```
(Routing)(Config)#ipv6 traffic-filter ip61 control-plane
```

10.9.4.1. no ipv6 traffic-filter

This command removes an IPv6 ACL identified by name from the interface(s) in a given direction.

Syntax	no ipv6 traffic-filter <name> {in|vlan vlan-id in} [sequence 1-4294967295]
Command Mode	Interface Config

Example: The following shows an example of the command.

```
(Routing) (Config)#no ipv6 traffic-filter ip61 control-plane
```

10.9.5. 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.

Syntax	show ipv6 access-lists [name]
Command Mode	Privileged EXEC

Term	Definition
Rule Number	The ordered rule number identifier defined within the IPv6 ACL.

Term	Definition
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.
Flow Label	The value specified for IPv6 Flow Label.
Assign Queue	The queue identifier to which packets matching this rule are assigned.
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 IPv6 ACL rule has referenced a time range.
Committed Rate	The committed rate defined by the rate-limit attribute.
Committed Burst Size	The committed burst size defined by the rate-limit attribute.
Rule Status	Status (Active/Inactive) of the IPv6 ACL rule.

Example: The following shows example CLI display output for the command.

```
(Routing) #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
```

10.10. 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.

10.10.1. 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. A 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.

When setting multiple entry, only Periodic time is included into Absolute time and clock time, the time-range will be active status .

When you successfully execute this command, the CLI mode changes to Time-Range admin mode.

Default	disabled
Syntax	time-range
Command Mode	Global Config

When you successfully execute this command, the CLI mode changes to identifie by name.

Syntax	time-range [name]
Command Mode	Global Config

10.10.1.1. no time-range

This command deletes a time-range identified by name.

Syntax	no time-range name
Command Mode	Global Config

10.10.2. 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.

Syntax	absolute {[start time date] [end time date]}
Command Mode	Time-Range Config

10.10.2.1. no absolute

This command deletes the absolute time entry in the time range.

Syntax	no absolute
Command Mode	Time-Range Config

10.10.3. 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
- Weekends - 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.

Syntax	periodic {days-of-the-week time} to {[days-of-the-week] time}
Command Mode	Time-Range Config

10.10.3.1. no periodic

This command deletes a periodic time entry from a time range/

Syntax	no periodic {days-of-the-week time} to {[days-of-the-week] time}
Command Mode	Time-Range Config

10.10.4. 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.

Syntax	show time-range
Command Mode	Privileged EXEC

Parameter	Definition
Number of Time Ranges	Number of time ranges configured in the system.
Time Range Name	Name of the time range.
Time Range Status	Status of the time range (active/inactive)
Absolute start	Start time and day for absolute time entry.
Absolute end	End time and day for absolute time entry.
Periodic Entries	Number of periodic entries in a time-range.
Periodic start	Start time and day for periodic entry.
Periodic end	End time and day for periodic entry.

Chapter 11. Stacking commands

This chapter describes the stacking commands available on FASTPATH CLI.

The stacking commands chapter includes the following sections:

11.1. Dedicated Port Stacking

This section describes the commands you use to configure dedicated port stacking.

11.1.1. stack

This command sets the mode to Stack Global Config.

Syntax	stack
Command Mode	Global Config

11.1.2. member

This command configures a switch. The *unit* is the switch identifier of the switch to be added/removed from the stack. The *switchindex* is the index into the database of the supported switch types, indicating the type of the switch being preconfigured. The switch index is a 32-bit integer. This command is executed on the Management Unit/Stack Master.

Syntax	member unit switchindex
Command Mode	Stack Global Config

Switch index can be obtained by executing the show supported switchtype command in User EXEC or Privileged EXEC mode.

11.1.3. no member

This command removes a switch from the stack. The *unit* is the switch identifier of the switch to be removed from the stack. This command is executed on the Management Unit/Stack Master.

Syntax	member unit
Command Mode	Stack Global Config

11.1.4. switch priority

This command configures the ability of a switch to become the Management Unit/Stack Master. The *unit* is the switch identifier. The *value* is the preference parameter that allows the user specify priority of one backup switch over another. The range for priority is 0 to 15. The switch with the highest priority value will be chosen to become the Stack Master if the current Stack Master fails. The switch priority defaults to the hardware management preference value 1. Switches that do not have the hardware capability to become the Stack Master are not eligible for management.

Default	enable

Syntax	switch unit priority value
Command Mode	Global Config

11.1.5. switch renumber

This command changes the switch identifier for a switch in the stack. The *oldunit* is the current switch identifier on the switch whose indentifier is to be changed. The *newunit* is the updated value of the switch identifier. Upon execution, the switch will be configured with the configuration information for the new switch, if any. The old switch configuration information will be retained, however the old switch will be operationally unplugged. This command is executed on the Stack Master.

If the Stack Master is renumbered, then the running configuration is no longer applied (i.e. the stack acts as if the configuration had been cleared).

Syntax	switch oldunit renumber newunit
Command Mode	Global Config

11.1.6. movemanagement

This command moves the Management Unit/Stack Master functionality from one switch to another. The *fromunit* is the switch identifier on the current Stack Master. The *tounit* is the switch identifier on the new Stack Master. Upon execution, the entire stack (including all interfaces in the stack) is unconfigured and reconfigured with the configuration on the new Stack Master. After the reload is complete, all stack management capability must be performed on the new Stack Master. To preserve the current configuration across a stack move, execute the **copy system: running-config nvram:startup-config** (in Privileged EXEC) command before performing the stack move. A stack move causes all routes and Layer 2 address to be lost. This command is executed on Management Unit/Stack Master. The system prompts you to confirm the management move.

Syntax	movemanagement fromunit tounit
Command Mode	Stack Global Config

11.1.7. standby

Use this command to configure a unit as a Standby Management Unit (STBY).

The Standby Management Unit cannot be the current Management Unit. The Standby Unit should be a management-capable unit.

Syntax	standby unit
Command Mode	Stack Global Config

11.1.8. no standby

The no form of this command allows the application to run the auto Standby Management Unit logic.

Syntax	no standby
Command Mode	Stack Global Config

11.1.9. show switch

This command displays information about all units in the stack or a single unit when you specify the unit value.

Syntax	show switch [unit]
Command Mode	Privileged EXEC

Term	Definition
Switch	The unit identifier assigned to the switch

When you do not specify a value for *unit*, the following information appears:

Term	Definition
Management Status	Indicates whether the switch is the Management Unit/Stack Master, a stack member, a configured Standby switch, an operational Standby switch, or the status is unassigned.
Preconfigured Model Identifier	The model identifier of a preconfigured switch ready to join the stack. The Model Identifier is a 32-character field assigned by the device manufacturer to identify the device.
Plugged-in Model Identifier	The model identifier of the switch in the stack. Model Identifier is a 32-character field assigned by the device manufacturer to identify the device.
Switch Status	The switch status. Possible values for this state are: **OK**, **Unsupported**, **Code Mismatch**, **Config Mismatch**, or **Not Present**. A mismatch indicates that a stack unit is running a different version of the code, SDM template, or configuration than the Management Unit/Stack Master. If there is a Stacking Firmware Syncronization operation in progress status is shown as **Updating Code**.
Code Version	The detected version of code on this switch.

Example: The following shows example CLI output for the command.

```
(Aurora 100-52)# show switch
```

```
    Management Standby   Preconfig      Plugged-in     Switch  Code
SW  Switch     Status    Model ID       Model ID       Status  Version
```

```
--- ---------- --------- -------------- -------------- ------- --------
1   Stack Mbr  Oper Stby Aurora 100-28P Aurora 100-28P OK      1.0.21
2   Stack Ms             Aurora 100-52  Aurora 100-52  OK      1.0.21
```

When you specify a value for *unit*, the following information appears.

Term	Definition
Management Status	Indicates whether the switch is the Management Unit/Stack Master, a stack member, a configured Standby switch, an operational Standby switch, or the status is unassigned.
Hardware Management Preference	The hardware management preference of the switch. The hardware managemente preference can be disabled of unassigned.
Admin Management Preference	The administrative management preference value assigned to the swtich. This preference value indicates how likely the switch is to be chosen as the new Management Unit/Stack Master.
Switch Type	The 32-bit numeric switch type.
Model Identifier	The model identifier for this switch. The model identifier is a 32-character field assigned by the device manufacturer to identify the device.
Switch Status	The switch status. Possible values are **OK**, **Unsupported**, **Code Mismatch**, **Config Mismatch**, or **Not Present**.
Switch Description	The switch description.
Expected Code Type	The expected code type.
Expected Code Version	The expected code version.
Detected Code Version	The version of code running on this switch. If the switch is not present and the data is from preconfiguration, then the code version is "Empty".
Detected Code in Flash	The version of code that is currently stored in FLASH memory on the switch. Tis code executes after the switch is reset. If the switch is not present and the data is from preconfiguration, then the code version is "None".
SFS Last Attempts Staus	The stack firmware syncronization status in the last attempt for the specified unit.
Serial Number	The serial number for the specified unit.
Up Time	The system up time.

11.1.10. show supported switchtype

This command displays information about all supported switch types or a specific switch type.

Syntax	show supported switchtype [switchindex]
Command Mode	User EXEC / Privileged EXEC

11.2. Stack Port Commands

This section describes the commands you use to view and configure stack port information.

11.2.1. stack-port

This command sets stacking per port or range of ports to either *stack* or *ethernet* mode.

Default	ethernet
Syntax	stack-port unit/slot/port [{ethernet | stack}]
Command Mode	Stack Global Config

11.2.2. show stack-port

This command displays summary stack-port information for all interfaces.

Syntax	show stack-port
Command Mode	Privileged EXEC

For each interface:

Term	Definition
Unit	The unit number.
Interface	The slot and port number.
Configured Stack Mode	Stack of Ethernet.
Running Stack Mode	Stack or Ethernet.
Link Status	Status of the link.
Link Speed	Speed (Gbps) of the stack port link.

11.2.3. show stack-port counters

This command displays summary data counter information for all interfaces.

Syntax	show stack-port counters
Command Mode	Privileged EXEC

11.2.4. show stack-port diag

This command shows stack port diagnostics for each port and is only intended for Field Application Engineers (FAEs) and developers. An FAE will advise on the necessity to run this command and capture this information.

Syntax	show stack-port diag
Command Mode	Privileged EXEC

11.2.5. show stack-port stack-path

This command displays the route a packet will take to reach the destination.

Syntax	show stack-port stack-path {1-6 | all}
Command Mode	Privileged EXEC

11.3. Stack Firmware Syncronization Commands

Stack Firmware Syncronization (SFS) provides the ability to automatically syncronize firmware for all stack memebers. If a unit joins the stack and its firmware version is different from the version running on the stack master, the SFS feature can either upgrade or downgrade the firmware on the mismatched stack member. There is no attempt to syncronize the stack to the latest firmware in the stack.

11.3.1. boot auto-copy-sw

Use this command to enable the Stack Firmware Syncronization feature on the stack.

Default	Disabled
Syntax	boot auto-copy-sw
Command Mode	Privileged EXEC

11.3.2. no boot auto-copy-sw

Use this command to disable the SFS feature on the stack.

Syntax	no boot auto-copy-sw
Command Mode	Privileged EXEC

11.3.3. boot auto-copy-sw trap

Use this command to enable the sending of SNMP traps related to the SFS feature.

Default	Enabled
Syntax	boot auto-copy-sw trap
Command Mode	Privileged EXEC

11.3.4. no boot auto-copy-sw trap

Use this command to disable the sending of SNMP traps related to the SFS feature.

Syntax	no boot auto-copy-sw trap
Command Mode	Privileged EXEC

11.3.5. boot auto-copy-sw allow-downgrade

Use this command to allow the stack master to downgrade the firmware version on the stack member if the firmware version on the stack master is older than the firmware version on the member.

Default	Enabled
Syntax	boot auto-copy-sw allow-downgrade
Command Mode	Privileged EXEC

11.3.6. no boot auto-copy-sw allow-downgrade

Use this command to prevent the stack master from downgrading the firmware version on a stack member.

Syntax	no boot auto-copy-sw allow-downgrade
Command Mode	Privileged EXEC

11.3.7. show auto-copy-sw

Use this command to display SFS configuration status information.

Syntax	show auto-copy-sw
Command Mode	Privileged EXEC

Term	Definition
Syncronization	Shows whether the SFS feature is enabled.
SNMP Trap Status	Shows whether the stack will send traps for SFS events.
Allow downgrade	Shows whether the stack master is permitted to downgrade the firmware version of a stack member.