ExtremeSwitching 200 Series: Command Reference Guide

122040-03 Rev. 02

Published February 2019

Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, please see:
www.extremenetworks.com/company/legal/trademarks

Software Licensing

Some software files have been licensed under certain open source or third-party licenses. End-user license agreements and open source declarations can be found at:
www.extremenetworks.com/support/policies/software-licensing

Support

For product support, phone the Global Technical Assistance Center (GTAC) at 1-800-998-2408 (toll-free in U.S. and Canada) or +1-408-579-2826. For the support phone number in other countries, visit: http://www.extremenetworks.com/support/contact/

For product documentation online, visit: https://www.extremenetworks.com/documentation/

Table of Contents

Preface

This section discusses the conventions used in this guide, ways to provide feedback, additional help, and other Extreme Networks publications.

Text Conventions

The following tables list text conventions that are used throughout this guide.

Table 1: Notice Icons

Icon	Notice Type	Alerts you to...
	General Notice	Helpful tips and notices for using the product.
	Note	Important features or instructions.
	Caution	Risk of personal injury, system damage, or loss of data.
	Warning	Risk of severe personal injury.
New!	New Content	Displayed next to new content. This is searchable text within the PDF.

Table 2: Text Conventions

Convention	Description
`Screen displays`	This typeface indicates command syntax, or represents information as it appears on the screen.
The words **enter** and **type**	When you see the word "enter" in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says "type."
[Key] names	Key names are written with brackets, such as **[Return]** or **[Esc]**. If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press **[Ctrl]**+**[Alt]**+**[Del]**
Words in italicized type	Italics emphasize a point or denote new terms at the place where they are defined in the text. Italics are also used when referring to publication titles.

Providing Feedback to Us

We are always striving to improve our documentation and help you work better, so we want to hear from you! We welcome all feedback but especially want to know about:

- Content errors or confusing or conflicting information.
- Ideas for improvements to our documentation so you can find the information you need faster.
- Broken links or usability issues.

If you would like to provide feedback to the Extreme Networks Information Development team about this document, please contact us using our short online feedback form. You can also email us directly at documentation@extremenetworks.com.

Getting Help

If you require assistance, contact Extreme Networks using one of the following methods:

Extreme Portal	Search the GTAC (Global Technical Assistance Center) knowledge base, manage support cases and service contracts, download software, and obtain product licensing, training, and certifications.
The Hub	A forum for Extreme Networks customers to connect with one another, answer questions, and share ideas and feedback. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.
Call GTAC	For immediate support: 1-800-998-2408 (toll-free in U.S. and Canada) or +1 408-579-2826. For the support phone number in your country, visit: www.extremenetworks.com/support/contact

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number and/or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any action(s) already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

Subscribing to Service Notifications

You can subscribe to email notifications for product and software release announcements, Vulnerability Notices, and Service Notifications.

1 Go to www.extremenetworks.com/support/service-notification-form.
2 Complete the form with your information (all fields are required).
3 Select the products for which you would like to receive notifications.

Note
You can modify your product selections or unsubscribe at any time.

4 Click **Submit**.

Extreme Networks Documentation

To find Extreme Networks product guides, visit our documentation pages at:

Current Product Documentation	www.extremenetworks.com/documentation/

Archived Documentation (for earlier versions and legacy products)	www.extremenetworks.com/support/documentation-archives/
Release Notes	www.extremenetworks.com/support/release-notes

Open Source Declarations

Some software files have been licensed under certain open source licenses. More information is available at: www.extremenetworks.com/support/policies/software-licensing/.

1 Using the Command-Line Interface

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

This chapter describes the CLI syntax, conventions, and modes.

Command Syntax

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

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

`network parms ipaddr netmask [gateway]`

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

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

- Format shows the command keywords and the required and optional parameters.
- Mode identifies the command mode you must be in to access the command.

- Default shows the default value, if any, of a configurable setting on the device.

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

Command Conventions

The parameters for a command might include mandatory values, optional values, or keyword choices. Parameters are order-dependent. Table 3 describes the conventions this document uses to distinguish between value types.

Table 3: Parameter Conventions

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

Common Parameter Values

Parameter values might be names (strings) or numbers. To use spaces as part of a name parameter, enclose the name value in double quotes. For example, the expression “System Name with Spaces” forces the system to accept the spaces. Empty strings (“”) are not valid user-defined strings. Table 4 describes common parameter values and value formatting.

Table 4: Parameter Descriptions

Parameter	Description
ipaddr	This parameter is a valid IP address. You can enter the IP address in the following formats: a (32 bits) a.b (8.24 bits) a.b.c (8.8.16 bits) a.b.c.d (8.8.8.8) In addition to these formats, the CLI accepts decimal, hexadecimal and octal formats through the following input formats (where n is any valid hexadecimal, octal or decimal number): 0xn (CLI assumes hexadecimal format.) 0n (CLI assumes octal format with leading zeros.) n (CLI assumes decimal format.)
ipv6-address	FE80:0000:0000:0000:020F:24FF:FEBF:DBCB, or FE80:0:0:0:20F:24FF:FEBF:DBCB, or FE80::20F24FF:FEBF:DBCB, or FE80:0:0:0:20F:24FF:128:141:49:32 For additional information, refer to RFC 3513.

Table 4: Parameter Descriptions (continued)

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

unit/slot/port Naming Convention

200 Series software references physical entities such as cards and ports by using a unit/slot/port naming convention. The 200 Series 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 5: 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. The value of logical slot numbers depend on the type of logical interface and can vary from platform to platform.
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 6: Type of Ports

Port Type	Description
Physical Ports	The physical ports for each slot are numbered sequentially starting from one/ For example, port 1 on slot 0 (an internal port) for a stand alone (nonstacked) switch is 1/0/1, port 2 is 1/0/2, port 3 is 1/0/3, and so on.
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.

Note

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

Using the "No" Form of a Command

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

Executing Show Commands

All show commands can be issued from any configuration mode (for example, Global Configuration, Interface Configuration, or VLAN Configuration). The show commands provide information about system and feature-specific configuration, status, and statistics. Previously, show commands could be issued only in User EXEC or Privileged EXEC modes.

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 the information of desired importance. The CLI Output Filtering feature allows the user, when executing CLI show display commands, to optionally specify 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
  - Supports enabling/disabling paginated output for all show CLI commands. When disabled, output is displayed in its entirety. When enabled, output is displayed page-by-page such that

content does not scroll off the terminal screen until the user presses a key to continue. --More-- or (q)uit is displayed at the end of each page.

- When pagination is enabled, press the return key to advance a single line, press q or Q to stop pagination, or press any other key to advance a whole page. These keys are not configurable.

Note

Although some 200 Series 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 (for example, interface 0/1) with a configurable end-of-section delimiter.

    String matching should be case insensitive.

    Pagination, when enabled, also applies to filtered output.

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 (for example, "interface 0/1") with a configurable end-of-section delimiter.

String matching should be case insensitive.

Pagination, when enabled, also applies to filtered output.

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

```
(Extreme 220) (Routing) #show running-config ?
<cr>                          Press enter to execute the command.
|                             Output filter options.
<scriptname>                  Script file name for writing active configuration.
all                           Show all the running configuration on the switch.
interface                             Display the running configuration for specified
interface on the switch.
(Extreme 220) (Routing) #show running-config | ?
begin                     Begin with the line that matches
exclude                   Exclude lines that matches
include                   Include lines that matches
section                   Display portion of lines
```

For new commands for the feature, see CLI Output Filtering Commands on page 137.

Command Modes

The CLI groups commands into modes according to the command function. Each of the command modes supports specific 200 Series software commands. The commands in one mode are not available until you switch to that particular mode, with the exception of the User EXEC mode commands. You can execute the User EXEC mode commands in the Privileged EXEC mode.

The command prompt changes in each command mode to help you identify the current mode. Table 7 on page 14 describes the command modes and the prompts visible in that mode.

Note
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 Router Command Mode.

Note
As shown in Table 7, most command prompts begin with `Extreme nnn` where *nnn* is the switch's model number – for example, `Extreme 220`.

Table 7: CLI Command Modes

Command Mode	Prompt	Mode Description
User EXEC	Extreme *nnn*>	Contains a limited set of commands to view basic system information.
Privileged EXEC	Extreme *nnn*#	Allows you to issue any `EXEC` command, enter the VLAN mode, or enter the Global Configuration mode.
Global Config	Extreme *nnn* (Config)#	Groups general setup commands and permits you to make modifications to the running configuration.
VLAN Config	Extreme *nnn* (Vlan)# or Extreme *nnn* (Vlan *vlan_id*)#	Groups all the VLAN commands.
Interface Config	Extreme *nnn* (Interface *unit/slot/port*)# Extreme *nnn* (Interface Loopback *id*)# Extreme *nnn* (Interface Tunnel *id*)# Extreme *nnn* (Interface *unit/slot/port (startrange)-unit/slot/port (endrange)*)#	Manages the operation of one or more interfaces 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 set of interfaces or a range of interfaces. For example: • `Extreme nnn (Interface 1/0/1,1/0/3) #` manages interfaces 1/0/1 and 1/0/3. • `Extreme nnn (Interface 1/0/1-1/0/4) #` manages the range of interfaces from 1/0/1 through 1/0/4.
	Extreme *nnn* (Interface vlan *vlan-id*)#	Enters VLAN routing interface configuration mode for the specified VLAN ID.

Table 7: CLI Command Modes (continued)

Command Mode	Prompt	Mode Description
Interface LAG Config	Extreme *nnn* (Interface lag *lag-intf-num*)#	Enters LAG interface configuration mode for the specified LAG.
Line Console	Extreme *nnn* (config-line)#	Contains commands to configure outbound telnet settings and console interface settings, as well as to configure console login/enable authentication.
Line SSH	Extreme *nnn* (config-ssh)#	Contains commands to configure SSH login/ enable authentication.
Line Telnet	Extreme *nnn* (config-telnet)#	Contains commands to configure telnet login/ enable authentication.
AAA IAS User Config	Extreme *nnn* (Config-IAS-User)#	Allows password configuration for a user in the IAS database.
Mail Server Config	Extreme *nnn* (Mail-Server)#	Allows configuration of the email server.
Policy Map Config	Extreme *nnn* (Config-policy-map)#	Contains the QoS Policy-Map configuration commands.
Policy Class Config	Extreme *nnn* (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	Extreme *nnn* (Config-class-map)#	Contains the QoS class map configuration commands for IPv4.
Ipv6_Class-Map Config	Extreme *nnn* (Config-class-map)#	Contains the QoS class map configuration commands for IPv6.
Router OSPFv3 Config	Extreme *nnn* (Config rtr)#	Contains the OSPFv3 configuration commands.
Router RIP Config	Extreme *nnn* (Config-router)#	Contains the RIP configuration commands.
Route Map Config	Extreme *nnn* (config-route-map)#	Contains the route map configuration commands.
IPv6 Address Family Config	Extreme *nnn* (Config-router-af)#	Contains the IPv6 address family configuration commands.
Peer Template Config	(Config-rtr-tmplt)#	Contains the BGP peer template configuration commands.
RADIUS Dynamic Authorization Config	(Config-radius-da)	Contains the RADIUS Dynamic Authorization commands.
MAC Access-list Config	Extreme *nnn* (Config-mac-access-list)#	Allows you to create a MAC Access-List and to enter the mode containing MAC Access-List configuration commands.
IPv4 Access-list Config	Extreme *nnn* (Config-ipv4-acl)#	Allows you to create an IPv4 named or extended Access-List and to enter the mode containing IPv4 Access-List configuration commands.
IPv6Access-list Config	Extreme *nnn* (Config-ipv6-acl)#	Allows you to create an IPv6 Access-List and to enter the mode containing IPv6 Access-List configuration commands.

Table 7: CLI Command Modes (continued)

Command Mode	Prompt	Mode Description
Management Access-list Config	Extreme *nnn* (config-macal)#	Allows you to create a Management Access-List and to enter the mode containing Management Access-List configuration commands.
TACACS Config	Extreme *nnn* (Tacacs)#	Contains commands to configure properties for the TACACS servers.
User-Group Configuration Mode	Extreme *nnn* (config-usergroup)	Contains user group commands
Task-Group Configuration Mode	Extreme *nnn* (config-taskgroup)	Contains task group commands
DHCP Pool Config	Extreme *nnn* (Config dhcp-pool)#	Contains the DHCP server IP address pool configuration commands.
DHCPv6 Pool Config	Extreme *nnn* (Config dhcp6-pool)#	Contains the DHCPv6 server IPv6 address pool configuration commands.
Stack Global Config Mode	Extreme *nnn* (Config stack)#	Allows you to access the Stack Global Config Mode.
ARP Access-List Config Mode	Extreme *nnn* (Config-arp-access-list)#	Contains commands to add ARP ACL rules in an ARP Access List.
Support Mode	Extreme *nnn* (Support)#	Allows access to the support commands, which should only be used by the manufacturer's technical support personnel as improper use could cause unexpected system behavior and/or invalidate product warranty.

Table 8 explains how to enter or exit each mode. To exit a mode and return to the previous mode, enter exit. To exit to Privileged EXEC mode, press **[Ctrl]+[Z]**.

Note
Pressing **[Ctrl]+[Z]** from Privileged EXEC mode exits to User EXEC mode. To exit User EXEC mode, enter `logout`.

Table 8: 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 `enable`.
Global Config	From the Privileged EXEC mode, enter `configure`.
VLAN Config	From the Privileged EXEC mode, enter `vlan database` or `vlan vlan_id`.

Table 8: CLI Mode Access and Exit (continued)

Command Mode	Access Method
Interface Config	From the Global Config mode, enter: `interface` *`unit/slot/port`* or `interface loopback` *`id`* or `interface tunnel` *`id`* `interface` *`unit1/slot1/port1,unit2/slot2/port2,...`* (to manage more than one interface) `interface` *`unit1/slot1/port1-unit2/slot2/port2-`* (to manage a range of interfaces) `interface vlan` *`vlan-id`*
Interface LAG Config	From the Global Config mode, enter `interface lag lag-intf-num`
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-Class-Map Config	From the Policy Map mode enter `class`.
Class-Map Config	From the Global Config mode, enter `class-map`, and specify the optional keyword **`ipv4`** to specify the Layer 3 protocol for this class. See class-map on page 599 for more information.
Ipv6-Class-Map Config	From the Global Config mode, enter `class-map` and specify the optional keyword **`ipv6`** to specify the Layer 3 protocol for this class. See class-map on page 599 for more information.
Router RIP Config	From the Global Config mode, enter `router rip`.
Route Map Config	From the Global Config mode, enter `-route-map` map-tag.
IPv6 Address Family Config	From the BGP Router Config mode, enter `address-family ipv6`.
Peer Template Config	From the BGP Router Config mode, enter `template peer` name to create a BGP peer template and enter Peer Template Configuration mode.
MAC Access-list Config	From the Global Config mode, enter `mac access-list extended name`.
IPv4 Access-list Config	From the Global Config mode, enter `ip access-list` name.
IPv6 Access-list Config	From the Global Config mode, enter `ipv6 access-list` name.
Management Access-list Config	From the Global Config mode, enter `management access-list` 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.
User-Group Configuration Mode	From the Global Config mode, enter the `usergroup` *`usergroup-name`* command.

Table 8: CLI Mode Access and Exit (continued)

Command Mode	Access Method
Task-Group Configuration Mode	From the Global Config mode, enter the `taskgroup` *`taskgroup-name`* command.
DHCP Pool Config	From the Global Config mode, enter the `ip dhcp pool` *`pool-name`* command.
DHCPv6 Pool Config	From the Global Config mode, enter the `ip dhcpv6 pool` *`pool-name`* command.
Stack Global Config Mode	From the Global Config mode, enter the `stack` command.
ARP Access-List Config Mode	From the Global Config mode, enter the `arp access-list` command.
Support Mode	From the Privileged EXEC mode, enter `support`. The `support` command is available only if the `techsupport enable` command has been issued.

Command Completion and Abbreviation

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

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

CLI Error Messages

If you enter a command and the system is unable to execute it, an error message appears. Table 9 describes the most common CLI error messages.

Table 9: CLI Error Messages

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

CLI Line-Editing Conventions

Table 10 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 10: CLI Editing Conventions

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

Using CLI Help

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

```
(Extreme 220) >?
enable                    Enter into user privilege mode.
help                      Display help for various special keys.
logout                    Exit this session. Any unsaved changes are lost.
password                            Change an existing user's password.
ping                      Send ICMP echo packets to a specified IP address.
quit                      Exit this session. Any unsaved changes are lost.
show                      Display Switch Options and Settings.
telnet                    Telnet to a remote host.
```

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

```
(Extreme 220) #network ?
ipv6                    Configure IPv6 parameters for system network.
javamode                Enable/Disable.
mac-address             Configure MAC Address.
mac-type                Select the locally administered or burnedin MAC
                        address.
mgmt_vlan               Configure the Management VLAN ID of the switch.
parms                   Configure Network Parameters of the device.
protocol                Select DHCP, BootP, or None as the network config
                        protocol.
```

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

```
(Extreme 220) (Routing) #network parms ?
<ipaddr>                Enter the IP Address.
none                    Reset IP address and gateway on management interface
```

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:

```
(Extreme 220) #show m?
mac                     mac-addr-table          mac-address-table
mail-server             mbuf                    monitor
```

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 (Dynamic Host Configuration Protocol)* server on your network. For more information, see Network Interface Commands on page 37.

2 Stacking Commands

This chapter describes the stacking commands available in the 200 Series CLI.

Caution

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

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

Note

The Primary Management Unit is the unit that controls the stack.

Note

Only 220 switches can be stacked.

Dedicated Port Stacking

This section describes the commands used to configure dedicated port stacking.

stack

This command sets the mode to Stack Global Config.

Format	`stack`
Mode	Global Config

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 Primary Management Unit.

Format	`member` *`unit switchindex`*
Mode	Stack Global Config

Note
Switch index can be obtained by executing the show supported switchtype command in User EXEC or Privileged EXEC mode.

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 Primary Management Unit.

Format	`no member` *`unit`*
Mode	Stack Global Config

switch priority

This command configures the ability of a switch to become the Primary Management Unit. The unit is the switch identifier. The value is the preference parameter that allows the user to specify, priority of one backup switch over another. The range for priority is 1 to 15. The switch with the highest priority value will be chosen to become the Primary Management Unit if the active Primary Management Unit fails. The switch priority defaults to the hardware management preference value 1. Switches that do not have the hardware capability to become the Primary Management Unit are not eligible for management.

Default	enabled
Format	`switch` *`unit`* `priority` *`value`*
Mode	Global Config

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 identifier 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 Primary Management Unit.

Note
If the management unit is renumbered, then the running configuration is no longer applied (that is, the stack acts as if the configuration had been cleared).

Format	`switch` *`oldunit`* `renumber` *`newunit`*
Mode	Global Config

movemanagement

This command moves the Primary Management Unit functionality from one switch to another. The fromunit is the switch identifier on the current Primary Management Unit. The tounit is the switch identifier on the new Primary Management Unit. Upon execution, the entire stack (including all interfaces in the stack) is unconfigured and reconfigured with the configuration on the new Primary Management Unit. After the reload is complete, all stack management capability must be performed on the new Primary Management Unit. 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 addresses to be lost. This command is executed on the Primary Management Unit. The system prompts you to confirm the management move.

Format	`movemanagement` *`fromunit tounit`*
Mode	Stack Global Config

standby

Use this command to configure a unit as a Standby Management Unit (STBY).

Note
The Standby Management Unit cannot be the current Management Unit.

Format	`standby` *`unit number`*
Mode	Stack Global Config

Parameter	Description
`unit number`	The unit number which is to be the Standby Management Unit. Must be a valid unit number.

no standby

The no form of this command allows the application to run the auto Standby Management Unit logic.

Format	`no standby`
Mode	Stack Global Config

slot

This command configures a slot in the system. The unit/slot is the slot identifier of the slot. The cardindex is the index into the database of the supported card types, indicating the type of the card being preconfigured in the specified slot. The card index is a 32-bit integer. If a card is currently present in the slot that is unconfigured, the configured information will be deleted and the slot will be reconfigured with default information for the card.

Format	`slot unit/slot cardindex`
Mode	Global Config

Note
Card index can be obtained by executing show supported cardtype command in User EXEC or Privileged EXEC mode.

no slot

This command removes configured information from an existing slot in the system.

Format	`no slot unit/slot cardindex`
Mode	Global Config

Note
Card index can be obtained by executing show supported cardtype command in User EXEC or Privileged EXEC mode.

set slot disable

This command configures the administrative mode of the slot(s). If you specify [all], the command is applied to all slots, otherwise the command is applied to the slot identified by unit/slot.

If a card or other module is present in the slot, this administrative mode will effectively be applied to the contents of the slot. If the slot is empty, this administrative mode will be applied to any module that is inserted into the slot. If a card is disabled, all the ports on the device are operationally disabled and shown as “unplugged” on management screens.

Format	`set slot disable [unit/slot] | all]`
Mode	Global Config

no set slot disable

This command unconfigures the administrative mode of the slot(s). If you specify all, the command removes the configuration from all slots, otherwise the configuration is removed from the slot identified by unit/slot.

If a card or other module is present in the slot, this administrative mode removes the configuration from the contents of the slot. If the slot is empty, this administrative mode removes the configuration from any module inserted into the slot. If a card is disabled, all the ports on the device are operationally disabled and shown as “unplugged” on management screens.

Format	`no set slot disable [unit/slot] | all]`
Mode	Global Config

set slot power

This command configures the power mode of the slot(s) and allows power to be supplied to a card located in the slot. If you specify all, the command is applied to all slots, otherwise the command is applied to the slot identified by unit/slot.

Use this command when installing or removing cards. If a card or other module is present in this slot, the power mode is applied to the contents of the slot. If the slot is empty, the power mode is applied to any card inserted into the slot.

Format	`set slot power [unit/slot	all]`
Mode	Global Config

no set slot power

This command unconfigures the power mode of the slot(s) and prohibits power from being supplied to a card located in the slot. If you specify all, the command prohibits power to all slots, otherwise the command prohibits power to the slot identified by unit/slot.

Use this command when installing or removing cards. If a card or other module is present in this slot, power is prohibited to the contents of the slot. If the slot is empty, power is prohibited to any card inserted into the slot.

Format	`no set slot power [unit/slot	all]`
Mode	Global Config

reload (Stack)

This command resets the entire stack or the identified unit. The unit is the switch identifier. The system prompts you to confirm that you want to reset the switch.

Format	`reload [unit]`
Mode	Privileged EXEC

stack-status sample-mode

Use this command to configure global status management mode, sample size. The mode, sample size parameters are applied globally on all units in the stack. The default sampling mode of the operation is cumulative summing.

Note

This configuration command is implemented as part of serviceability functionality and therefore is not expected to be persistent across reloads. This configuration is never visible in the running configuration under any circumstances. It is the responsibility of the user to switch the sample mode on-demand as per the requirement. This configuration is applied to all the members that are part of the stack when the command is triggered. This configuration cannot play onto cards that are part of the stack at later point of the time.

Default	Cumulative Summing
Format	`stack-status sample-mode {`*`cumulative`* `|` *`history`*`} [`**`max-samples`** *`100 - 500`*`]`
Mode	Stack Global Config Mode

Parameter	Description
`sample-mode`	Mode of sampling
`cumulative`	Tracks the sum of received time stamp offsets cumulatively.
`history`	Tracks history of received timestamps
`max-samples`	Maximum number of samples to keep

The following command sets the sampling mode to cumulative summing.

```
(Extreme 220) (Routing) #configure
(Extreme 220) (Config) #stack
(Extreme 220) (Config-stack)# stack-status sample-mode cumulative
```

The following command sets the sampling mode to history and the sample size to default (that is, 300).

```
(Extreme 220) #configure
(Extreme 220) (Config) #stack
(Extreme 220) (Config-stack)#stack-status sample-mode history
```

The following command sets the sampling mode to history and sample size to 100.

```
(Extreme 220) #configure
(Extreme 220) (Config) (Config)#stack
(Extreme 220) (Config-stack)#stack-status sample-mode history max-samples 100
```

show slot

This command displays information about all the slots in the system or for a specific slot.

Format	`show slot` *`[unit/slot]`*
Mode	• User EXEC • Privileged EXEC

Column	Meaning
Slot	The slot identifier in a *`unit/slot`* format.
Slot Status	The slot is empty, full, or has encountered an error
Admin State	The slot administrative mode is enabled or disabled.
Power State	The slot power mode is enabled or disabled.
Configured Card Model Identifier	The model identifier of the card preconfigured in the slot. Model Identifier is a 32-character field used to identify a card.

Column	Meaning
Pluggable	Cards are pluggable or non-pluggable in the slot.
Power Down	Whether the slot can be powered down.

If you supply a value for unit/slot, the following additional information appears:

Column	Meaning
Inserted Card Model Identifier	The model identifier of the card inserted in the slot. Model Identifier is a 32-character field used to identify a card. This field is displayed only if the slot is full.
Inserted Card Description	The card description. This field is displayed only if the slot is full.
Configured Card Description	10BASE-T half duplex

show stack-status

Use this command to display the stack unit's received HB message timings, and the dropped/lost statistics for the specified unit.

Format	`show stack stack-status [1-n | all] [clear]`
Mode	Privileged EXEC

Column	Meaning
Current	Current time of heartbeat message reception
Average	Average time of heartbeat messages received
Min	Minimum time of heartbeat messages received
Max	Maximum time of heartbeat messages received
Dropped	Heartbeat message dropped/lost counter

This example dumps the stack unit heartbeat status information of the specified unit.

```
(Extreme 220) (Routing) #show stack-status
Stack Unit 1 Status
Sampling Mode: Cumulative Summing
-------------------------------------
Unit Current Average Min  Max  Dropped
-------------------------------------
```

show supported cardtype

This commands displays information about all card types or specific card types supported in the system.

Format	`show supported cardtype [cardindex]`
Mode	• User EXEC • Privileged EXEC

If you do not supply a value for cardindex, the following output appears:

Column	Meaning
Card Index (CID)	The index into the database of the supported card types. This index is used when preconfiguring a slot.
Card Model Identifier	The model identifier for the supported card type.

If you supply a value for cardindex, the following output appears:

Column	Meaning
Card Type	The 32-bit numeric card type for the supported card.
Model Identifier	The model identifier for the supported card type.
Card Description	The description for the supported card type.

show switch

This command displays switch status information about all units in the stack or a single unit when you specify the unit value.

Format	`show switch [unit]`
Mode	Privileged EXEC

Column	Meaning
Switch	The unit identifier assigned to the switch.

When you do not specify a value for unit, the following information appears:

Column	Meaning
Management Status	Whether the switch is the Primary Management Unit, 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, SDM 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. The SDM Mismatch status indicates that the unit joined the stack, but is running a different SDM template than the management unit. This status is temporary; the stack unit should automatically reload using the template running on the stack manager. If there is a Stacking Firmware Synchronization operation in progress status is shown as Updating Code.
Code Version	The detected version of code on this switch.

The following example shows CLI display output for the command.

```
(Extreme 220) (Config) #show switch
    Management  Standby    Preconfig     Plugged-in     Switch       Code
```

```
SW    Switch    Status     Model ID      Model ID       Status       Version
--- ---------- --------- ------------- ------------- ------------ -----------
1   Mgmt Sw               220-24t-10GE2    220-24t-10GE2    OK           1.1.1.10
2   Stack Mbr   Oper Stby 220-48t-10GE4    220-48t-10GE4    OK           1.1.1.10
```

When you specify a value for *unit*, the following information displays.

Column	Meaning
Management Status	Whether the switch is the Primary Management Unit, a stack member, or the status is unassigned.
Hardware Management Preference	The hardware management preference of the switch. The hardware management preference can be disabled or unassigned.
Admin Management Preference	The administrative management preference value assigned to the switch. This preference value indicates how likely the switch is to be chosen as the Primary Management Unit.
Switch Type	The 32-bit numeric switch type.
Model Identifier	The model identifier for this switch. 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, SDM Mismatch, STM 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 “None”.
Detected Code in Flash	The version of code that is currently stored in FLASH memory on the switch. This code executes after the switch is rebooted. If the switch is not present and the data is from preconfiguration, then the code version is “None”.
SFS Last Attempt Status	The stack firmware synchronization status in the last attempt for the specified unit.
Serial Number	The serial number for the specified unit.
Up Time	The system up time.

The following example shows CLI display output for the command.

```
(Extreme 220) (Config) #show switch 2
Switch.............................. 2
Management Status................... Stack Member
Hardware Management Preference.... Unassigned
Admin Management Preference....... Unassigned
Switch Type......................... 0xb1500005
Preconfigured Model Identifier.... 220-48t-10GE4
Plugged-in Model Identifier....... 220-48t-10GE4
Switch Status....................... OK
Switch Description.................. Extreme 220-Series 48GE, 4 10GbE SFP+ ports,
1 Fixed AC PSU, 1 RPS port, L3 Switching
Detected Code in Flash.............. 1.1.1.10
SFS Last Attempt Status............. None
Serial Number....................... 1648G-01431
Up Time............................. 1 days 19 hrs 44 mins 26 secs
```

show supported switchtype

This command displays information about all supported switch types or a specific switch type.

Format	`show supported switchtype [switchindex]`
Mode	User EXEC Privileged EXEC

If you do not supply a value for switchindex, the following output appears:

Column	Meaning
Switch Index (SID)	The index into the database of supported switch types. This index is used when preconfiguring a member to be added to the stack.
Model Identifier	The model identifier for the supported switch type.
Management Preference	The management preference value of the switch type.
Code Version	The code load target identifier of the switch type.

If you supply a value for switchindex, the following output appears:

Column	Meaning
Switch Type	The 32-bit numeric switch type for the supported switch.
Model Identifier	The model identifier for the supported switch type.
Switch Description	The description for the supported switch type.

Stack Port Commands

This section describes the commands used to view and configure stack port information.

stack-port

This command sets stacking per port or range of ports to either stack or ethernet mode.

Default	stack
Format	`stack-port unit/slot/port [{ethernet | stack}]`
Mode	Stack Global Config

show stack-port

This command displays summary stack-port information for all interfaces.

Format	`show stack-port`
Mode	Privileged EXEC

For Each Interface:

Column	Meaning
Unit	The unit number.
Interface	The slot and port numbers.
Configured Stack Mode	Stack or Ethernet.
Running Stack Mode	Stack or Ethernet.
Link Status	Status of the link.
Link Speed	Speed (Gbps) of the stack port link.

show stack-port counters

This command displays summary data counter information for all interfaces.

Format	`show stack-port counters [1-n | all]`
Mode	Privileged EXEC

Column	Meaning
Unit	The unit number.
Interface	The slot and port numbers.
Tx Data Rate	Trashing data rate in megabits per second on the stacking port.
Tx Error Rate	Platform-specific number of transmit errors per second.
Tx Total Errors	Platform-specific number of total transmit errors since power-up.
Rx Data Rate	Receive data rate in megabits per second on the stacking port.
Rx Error Rate	Platform-specific number of receive errors per second.
Rx Total Errors	Platform-specific number of total receive errors since power-up.
Link Flaps	The number of up/down events for the link since system boot up.

This example shows the stack ports and associated statistics of unit 2.

```
(Extreme 220) (Routing) #show stack-port counters 2
                  ------------TX---------------    ------------RX--------------  -----
                  Data      Error                   Data    Error
                  Rate      Rate         Total      Rate    Rate         Total   Link
Unit   Interface  (Mb/s)    (Errors/s)   Errors     (Mb/s)  (Errors/s)   Errors  Flaps
----   ---------  -------   ----------   ------     ------  ----------   ------  -----
2        0/53        0         0            0          0       0            0       0
2        0/54        0         0            0          0       0            0       0
2        0/55        0         0            0          0       0            0       0
2        0/56        0         0            0          0       0            0       0
(Extreme 220) (Routing) #
```

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. In verbose mode, the statistics and counters for RPC, transport, CPU, and transport RX/TX modules are displayed.

Format	`show stack-port diag [1-n | all] [verbose]`
Mode	Privileged EXEC

Column	Meaning
Unit	The unit number.
Interface	The slot and port numbers.
Diagnostic Entry1	80-character string used for diagnostics.
Diagnostic Entry2	80-character string used for diagnostics.
Diagnostic Entry3	80-character string used for diagnostics.
TBYT	Transmitted Bytes
TPKT	Transmitted Packets
TFCS	Transmit FCS Error Frame Counter
TERR	Transmit Error (set by system) Counter
RBYT	Received Bytes
RPKT	Received Packets
RFCS	Received FCS Error Frame Counter
RFRG	Received Fragment Counter
RJBR	Received Jabber Frame Counter
RUND	Received Undersize Frame Counter
ROVR	Received Oversized Frame Counter
RUNT	Received RUNT Frame Counter

This example displays the stack ports and associated statistics of specified unit or all units.

```
(Extreme 220) (Routing) #show stack-port diag 1
1 - 0/53:
RBYT:27ed9a7b RPKT:bca1b TBYT:28a0739e TPKT:c93ee
RFCS:0 RFRG:0 RJBR:0 RUND:0 RUNT:0
TFCS:0 TERR:0
1 - 0/54:
RBYT:8072ed RPKT:19a66 TBYT:aecfb80 TPKT:66e4d
RFCS:6e RFRG:4414 RJBR:0 RUND:c19 RUNT:af029b1
TFCS:0 TERR:0
1 - 0/55:
RBYT:0 RPKT:0 TBYT:ae8 TPKT:23
RFCS:0 RFRG:0 RJBR:0 RUND:0 RUNT:0
TFCS:0 TERR:0
1 - 0/56:
RBYT:0 RPKT:0 TBYT:ae8 TPKT:23
RFCS:0 RFRG:0 RJBR:0 RUND:0 RUNT:0
TFCS:0 TERR:0
Example 2: 'show stack-port diag [<1-n> | all] [verbose]' transport etc module statistics
of specified unit or all units.
In this example, It dumps RPC, Transport (ATP, Next Hop, and RLink), and CPU Transport
Rx/Tx modules Statistics of Unit 2.
(Extreme 220) (Routing) #show stack-port diag 2 verbose
```

```
---------------------------------------
HPC RPC statistics/counters from unit..2
---------------------------------------
Registered Functions.......................... 58
Client Requests............................... 0
Server Requests............................... 0
Server Duplicate Requests..................... 0
Server Replies................................ 0
Client Remote Tx.............................. 0
Client Remote Retransmit Count................ 0
Tx without Errors............................. 0
Tx with Errors................................ 0
Rx Timeouts................................... 0
Rx Early Exits................................ 0
Rx Out of Sync................................ 0
No Buffer..................................... 0
Collect Sem Wait Count........................ 0
Collect Sem Dispatch Count.................... 0
-------------------------------------
RPC statistics/counters from unit..2
-------------------------------------
Client RPC Requests Count..................... 3
Client RPC Reply Count........................ 0
Client RPC Fail to xmit Count................. 0
Client RPC Response Timedout Count............ 3
Client RPC Missing Requests................... 0
Client RPC Detach/Remove Count................ 0
Client RPC Current Sequence Number............ 3
Server RPC Request Count...................... 0
Server RPC Reply Count........................ 0
Server RPC Processed Transactions............. 0
Server RPC Received Wrong Version Req......... 0
Server RPC No Handlers........................ 0
Server RPC Retry Transmit Count............... 0
Server RPC Repetitive Tx Errors............... 0
-------------------------------------
ATP statistics/counters from unit..2
-------------------------------------
Transmit Pending Count........................ 2
Current number of TX waits.................... 2
Rx transactions created....................... 145
Rx transactions freed......................... 145
Rx transactions freed(raw).................... 0
--More-- or (q)uitATP: TX timeout, seq 74. f:cc cli 778. to 1 tx cnt 21.
Tx transactions created....................... 290
BET Rx Dropped Pkts Count..................... 0
ATP Rx Dropped Pkts Count..................... 0
Failed to Add Key Pkt Count................... 0
Source Lookup Failure Count................... 0
Old Rx transactions Pkts drop Count........... 0
Nr of CPUs found in ATP communication......... 2
-----------------------------------------------
CPU Transport statistics/counters from unit..2
-----------------------------------------------
State Initialization.......................... Done
Rx Setup...................................... Done
Tx Setup...................................... Done
Tx CoS[0] Reserve............................. 100
Tx CoS[1] Reserve............................. 100
Tx CoS[2] Reserve............................. 100
Tx CoS[3] Reserve............................. 100
Tx CoS[4] Reserve............................. 60
Tx CoS[5] Reserve............................. 40
Tx CoS[6] Reserve............................. 20
```

```
Tx CoS[7] Reserve.............................. 0
Tx Pkt Pool Size............................... 200
Tx Available Pkt Pool Size..................... 198
Tx failed/error Count.......................... 0
Rx Pkt Pool Size............................... 8
----------------------------------------
Next Hop statistics/counters from unit..2
----------------------------------------
State Initialization........................... Done
Component Setup................................ Done
Thread Priority................................ 100
Rx Priority.................................... 105
Local CPU Key.................................. 00:24:81:d0:0f:c7
MTU Size....................................... 2048
Vlan Id........................................ 4094
CoS Id......................................... 7
Internal Priority for pkt transmission......... 7
Rx Pkt Queue Size.............................. 256
Tx Pkt Queue Size.............................. 64
Rx Pkt Dropped Count........................... 0
Tx Failed Pkt Count............................ 0
---------------------------------------
RLink statistics/counters from unit..2
---------------------------------------
State Initialization........................... Done
L2 Notify In Pkts.............................. 0
L2 Notify In Pkts discarded.................... 0
L2 Notify Out Pkts ............................ 0
L2 Notify Out Pkts discarded................... 0
Linkscan In Pkts............................... 0
Linkscan In Pkts discarded..................... 0
Linkscan Out Pkts ............................. 0
Linkscan Out Pkts discarded.................... 0
Auth/Unauth In Callbacks....................... 0
Auth/Unauth In Callbacks discarded............. 0
Auth/Unauth Out Callbacks...................... 0
Auth/Unauth Out Callbacks discarded............ 0
RX Tunnelling In Pkts.......................... 0
RX Tunnelling In Pkts discarded................ 0
RX Tunnelling Out Pkts......................... 0
RX Tunnelling Out Pkts discarded............... 0
OAM Events In.................................. 0
OAM Events In discarded........................ 0
OAM Events Out................................. 0
OAM Events Out discarded....................... 0
BFD Events In.................................. 0
BFD Events In discarded........................ 0
BFD Events Out................................. 0
BFD Events Out discarded....................... 0
Fabric Events In............................... 0
Fabric Events In discarded..................... 0
Fabric Events Out.............................. 0
Fabric Events Out discarded.................... 0
Scan Add Requests In........................... 0
Scan Del Requests In........................... 0
Scan Notify(Run Handlers) Out.................. 0
Scan Notify(Traverse Processing)............... 0
(Extreme 220) (Routing) #
```

show stack-port stack-path

This command displays the route a packet will take to reach the destination.

Format	`show stack-port stack-path {1-8 | all}`
Mode	Privileged EXEC

Stack Firmware Synchronization Commands

Stack Firmware Synchronization (SFS) provides the ability to automatically synchronize firmware for all stack members. If a unit joins the stack and its firmware version is different from the version running on the stack manager, the SFS feature can either upgrade or downgrade the firmware on the mismatched stack member. There is no attempt to synchronize the stack to the latest firmware in the stack.

boot auto-copy-sw

Use this command to enable the Stack Firmware Synchronization feature on the stack.

Default	Disabled
Format	`boot auto-copy-sw`
Mode	Privileged EXEC

no boot auto-copy-sw

Use this command to disable the Stack Firmware Synchronization feature on the stack

Format	`no boot auto-copy-sw`
Mode	Privileged EXEC

boot auto-copy-sw trap

Use this command to enable the sending of *SNMP (Simple Network Management Protocol)* traps related to the Stack Firmware Synchronization feature.

Default	Enabled
Format	`boot auto-copy-sw trap`
Mode	Privileged EXEC

no boot auto-copy-sw trap

Use this command to disable the sending of traps related to the Stack Firmware Synchronization feature.

Format	`no boot auto-copy-sw trap`
Mode	Privileged EXEC

boot auto-copy-sw allow-downgrade

Use this command to allow the stack manager to downgrade the firmware version on the stack member if the firmware version on the manager is older than the firmware version on the member.

Default	Enabled
Format	`boot auto-copy-sw allow-downgrade`
Mode	Privileged EXEC

no boot auto-copy-sw allow-downgrade

Use this command to prevent the stack manager from downgrading the firmware version of a stack member.

Format	`no boot auto-copy-sw allow-downgrade`
Mode	Privileged EXEC

show auto-copy-sw

Use this command to display Stack Firmware Synchronization configuration status information.

Format	`show auto-copy-sw`
Mode	Privileged EXEC

Column	Meaning
Synchronization	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 manager is permitted to downgrade the firmware version of a stack member.

3 Management Commands

This chapter describes the management commands available in the 200 Series CLI.

Caution

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

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

Network Interface Commands

This section describes the commands used to configure a logical interface for management access. To configure the management VLAN, see network mgmt_vlan on page 317.

enable (Privileged EXEC access)

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

Format	`enable`
Mode	User EXEC

do (Privileged EXEC commands)

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

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

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

```
(Extreme 220) #configure
(Extreme 220) (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)#
```

serviceport ip

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

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

serviceport protocol

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

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

serviceport protocol dhcp

This command enables the DHCPv4 client on a Service port. If the **client-id** optional parameter is given, the *DHCP* client messages are sent with the client identifier option.

Default	none
Format	`serviceport protocol dhcp [client-id]`
Mode	Privileged EXEC

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

The following shows an example of the command.

```
(Extreme 220) (Routing) # serviceport protocol dhcp client-id
```

network parms

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

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

network protocol

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

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

network protocol dhcp

This command enables the DHCPv4 client on a Network port. If the **client-id** optional parameter is given, the *DHCP* client messages are sent with the client identifier option.

Default	None
Format	`network protocol dhcp [client-id]`
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.

The following shows an example of the command.

```
(Extreme 220) (Routing) # network protocol dhcp client-id
```

network mac-address

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

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

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

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

network mac-type

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

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

no network mac-type

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

Format	`no network mac-type`
Mode	Privileged EXEC

network javamode

This command specifies whether the switch should allow access to the Java applet in the header frame of the web interface. When access is enabled, the Java applet can be viewed from the web interface. When access is disabled, users cannot view the Java applet.

Default	enabled
Format	`network javamode`
Mode	Privileged EXEC

no network javamode

This command disallows access to the Java applet in the header frame of the web interface. When access is disabled, the user cannot view the Java applet.

Format	`no network javamode`
Mode	Privileged EXEC

show network

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

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

Column	Meaning
Interface Status	The network interface status; it is always considered to be “up”.
IP Address	The IP address of the interface. The factory default value is 0.0.0.0.
Subnet Mask	The IP subnet mask for this interface. The factory default value is 0.0.0.0.
Default Gateway	The default gateway for this IP interface. The factory default value is 0.0.0.0.
IPv6 Administrative Mode	Whether enabled or disabled.
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.
Locally Administered MAC Address	If desired, a locally administered MAC address can be configured for in-band connectivity. To take effect, 'MAC Address Type' must be set to 'Locally Administered'. Enter the address as twelve hexadecimal digits (6 bytes) with a colon between each

Column	Meaning
	byte. Bit 1 of byte 0 must be set to a 1 and bit 0 to a 0, that is, byte 0 should have the following mask 'xxxx xx10'. The MAC address used by this bridge when it must be referred to in a unique fashion. We recommend that this be the numerically smallest MAC address of all ports that belong to this bridge. However it is only required to be unique. When concatenated with dot1dStpPriority a unique Bridge Identifier is formed which is used in the Spanning Tree Protocol.
MAC Address Type	The MAC address which should be used for in-band connectivity. The choices are the burned in or the Locally Administered address. The factory default is to use the burned in MAC address.
Configured IPv4 Protocol	The IPv4 network protocol being used. The options are bootp | dhcp | none.
Configured IPv6 Protocol	The IPv6 network protocol being used. The options are dhcp | none.
DHCPv6 Client DUID	The DHCPv6 client's unique client identifier. This row is displayed only when the configured IPv6 protocol is dhcp.
IPv6 Autoconfig Mode	Whether IPv6 Stateless address autoconfiguration is enabled or disabled.
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. See network protocol dhcp on page 39.

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

```
(admin) #show network
Interface Status.............................. 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
```

show serviceport

This command displays service port configuration information.

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

Column	Meaning
Interface Status	The network interface status. It is always considered to be up.
IP Address	The IP address of the interface. The factory default value is 0.0.0.0.

Column	Meaning
Subnet Mask	The IP subnet mask for this interface. The factory default value is 0.0.0.0.
Default Gateway	The default gateway for this IP interface. The factory default value is 0.0.0.0.
IPv6 Administrative Mode	Whether enabled or disabled. Default value is enabled.
IPv6 Address/Length	The IPv6 address and length. Default is Link Local format.
IPv6 Default Router	TheIPv6 default router address on the service port. The factory default value is an unspecified 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's unique client identifier. This row is displayed only when the configured IPv6 protocol is dhcp.
IPv6 Autoconfig Mode	Whether IPv6 Stateless address autoconfiguration is enabled or disabled.
Burned in MAC Address	The burned in MAC address used for in-band connectivity.
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 service port. See serviceport protocol on page 38.

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

```
(admin) #show serviceport
Interface Status.............................. Up
IP Address.................................... 10.230.3.51
Subnet Mask................................... 255.255.255.0
Default Gateway............................... 10.230.3.1
IPv6 Administrative Mode...................... Enabled
IPv6 Prefix is ............................... fe80::210:18ff:fe82:640/64
IPv6 Prefix is ............................... 2005::21/128
IPv6 Default Router is ....................... fe80::204:76ff:fe73:423a
Configured IPv4 Protocol ..................... DHCP
Configured IPv6 Protocol ..................... DHCP
DHCPv6 Client DUID ........................... 00:03:00:06:00:10:18:82:06:4C
IPv6 Autoconfig Mode.......................... Disabled
Burned In MAC Address......................... 00:10:18:82:06:4D
DHCP Client Identifier........................ 0fastpath-0010.1882.160C
```

Console Port Access Commands

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

configure (Global Config mode)

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

Format	`configure`
Mode	Privileged EXEC

line

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

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

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

The following shows an example of this command.

```
(Extreme 220) (Config)#line telnet
(Extreme 220)(config-telnet)#
```

serial baudrate

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

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

no serial baudrate

This command sets the communication rate of the terminal interface.

Format	`no serial baudrate`
Mode	Line Config

serial timeout

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

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

no serial timeout

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

Format	`no serial timeout`
Mode	Line Config

show serial

This command displays serial communication settings for the switch.

Format	`show serial`
Modes	• Privileged EXEC • User EXEC

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

Telnet Commands

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

ip telnet server enable

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

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

no ip telnet server enable

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

Format	`no ip telnet server enable`
Mode	Privileged EXEC

ip telnet port

This command configures the TCP port number on which the Telnet server listens for requests.

Default	23
Format	`ip telnet port` *`1-65535`*
Mode	Privileged EXEC

no ip telnet port

This command restores the Telnet server listen port to its factory default value.

Format	`no ip telnet port`
Mode	Privileged EXEC

telnet

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

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

transport input telnet

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

Note

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

Default	enabled
Format	`transport input telnet`
Mode	Line Config

no transport input telnet

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

Format	`no transport input telnet`
Mode	Line Config

transport output telnet

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

Default	enabled
Format	`transport output telnet`
Mode	Line Config

no transport output telnet

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

Format	`no transport output telnet`
Mode	Line Config

session-limit

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

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

no session-limit

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

Format	`no session-limit`
Mode	Line Config

session-timeout

This command sets the Telnet session timeout value, in minutes.

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

no session-timeout

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

Format	`no session-timeout`
Mode	Line Config

telnetcon maxsessions

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

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

no telnetcon maxsessions

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

Format	`no telnetcon maxsessions`
Mode	Privileged EXEC

telnetcon timeout

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

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

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

no telnetcon timeout

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

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

Format	`no telnetcon timeout`
Mode	Privileged EXEC

show telnet

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

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

Column	Meaning
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	Whether outbound Telnet sessions will be allowed.

show telnetcon

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

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

Column	Meaning
Remote Connection Login Timeout (minutes)	This object indicates the number of minutes a remote connection session is allowed to remain inactive before being logged off. May be specified as a number from 1 to 160. The factory default is 5.
Maximum Number of Remote Connection Sessions	This object indicates the number of simultaneous remote connection sessions allowed. The factory default is 5.
Allow New Telnet Sessions	New Telnet sessions will not be allowed when this field is set to no. The factory default value is yes.
Telnet Server Admin Mode	If Telnet Admin mode is enabled or disabled.
Telnet Server Port	The configured TCP port number on which the Telnet server listens for requests. (The default is 23.)

Secure Shell Commands

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

Note
The system allows a maximum of five SSH sessions.

ip ssh

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

Default	Disabled
Format	`ip ssh`
Mode	Privileged EXEC

ip ssh port

Use this command to configure the TCP port number on which the SSH server listens for requests. Valid port numbers are from 1–65535.

Default	22
Format	`ip ssh port` *`1-65535`*
Mode	Privileged EXEC

no ip ssh port

Use this command to restore the SSH server listen port to its factory default value.

Format	`no ip ssh port`
Mode	Privileged EXEC

ip ssh protocol

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

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

ip ssh server enable

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

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

no ip ssh server enable

This command disables the IP secure shell server.

Format	`no ip ssh server enable`
Mode	Privileged EXEC

sshcon maxsessions

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

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

no sshcon maxsessions

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

Format	`no sshcon maxsessions`
Mode	Privileged EXEC

sshcon timeout

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

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

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

no sshcon timeout

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

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

Format	`no sshcon timeout`
Mode	Privileged EXEC

show ip ssh

This command displays the SSH settings.

Format	`show ip ssh`
Mode	Privileged EXEC

Column	Meaning
Administrative Mode	This field indicates whether the administrative mode of SSH is enabled or disabled.
SSH Port	The SSH port.
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.

Column	Meaning
Keys Present	Whether the SSH RSA and DSA key files are present on the device.
Key Generation in Progress	Whether RSA or DSA key files generation is currently in progress.

Management Security Commands

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

crypto certificate generate

Use this command to generate a self-signed certificate for HTTPS. The generated RSA key for SSL has a length of 1024 bits. The resulting certificate is generated with a common name equal to the lowest IP address of the device and a duration of 365 days.

Format	`crypto certificate generate`
Mode	Global Config

no crypto certificate generate

Use this command to delete the HTTPS certificate files from the device, regardless of whether they are self-signed or downloaded from an outside source.

Format	`no crypto certificate generate`
Mode	Global Config

crypto key generate rsa

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

Format	`crypto key generate rsa`
Mode	Global Config

no crypto key generate rsa

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

Format	`no crypto key generate rsa`
Mode	Global Config

crypto key generate dsa

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

Format	`crypto key generate dsa`
Mode	Global Config

no crypto key generate dsa

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

Format	`no crypto key generate dsa`
Mode	Global Config

Hypertext Transfer Protocol Commands

This section describes the commands used to configure *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.

ip http accounting exec, ip https accounting 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 `aaa accounting` command (see aaa accounting on page 87).

Format	`ip {http|https} accounting exec {default|listname}`
Mode	Global Config

Parameter	Description
`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.

no ip http/https accounting exec

This command deletes the authorization method list.

Format	`no ip {http|https} accounting exec {default|listname}`
Mode	Global Config

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 (Remote Authentication Dial In User Service)* server is down.

Default	local
Format	`ip http authentication method1 [method2...]`
Mode	Global Config

Parameter	Description
method1 [method2...]	Specify at least one from the following: • **local**: Uses the local username database for authentication. • **none**: Uses no authentication. • **radius**: Uses the list of all RADIUS servers for authentication. • **tacacs**: Uses the list of all TACACS+ servers for authentication.

The following example configures the HTTP authentication.

```
(Extreme 220) (Config) # ip http authentication radius local
```

no ip http authentication

Use this command to return to the default.

Format	`no ip http authentication`
Mode	Global Config

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**
Format	`ip https authentication method1 [method2...]`
Mode	Global Config

Parameter	Description
local	Uses the local username database for authentication.
none	Uses no authentication.
radius	Uses the list of all RADIUS servers for authentication.
tacacs	Uses the list of all TACACS+ servers for authentication.

The following example configures HTTPS authentication.

```
(Extreme 220) (Config) # ip https authentication radius local
```

no ip https authentication

Use this command to return to the default.

Format	`no ip https authentication`
Mode	Global Config

ip http server

This command enables access to the switch through the web interface. When access is enabled, users can log in to the switch from the web interface. When access is disabled, users cannot log in to the switch's web server. Disabling the web interface takes effect immediately. All interfaces are affected.

Default	Enabled
Format	`ip http server`
Mode	Privileged EXEC

no ip http server

This command disables user access to the switch through the web interface.

Format	`no ip http server`
Mode	Privileged EXEC

ip http secure-server

This command enables the secure socket layer for secure HTTP.

Default	Disabled
Format	`ip http secure-server`
Mode	Privileged EXEC

no ip http secure-server

This command disables the secure socket layer for secure HTTP.

Format	`no ip http secure-server`
Mode	Privileged EXEC

ip http java

This command enables the web Java mode. The Java mode applies to both secure and unsecure web connections.

Default	Enabled
Format	`ip http java`
Mode	Privileged EXEC

no ip http java

This command disables the web Java mode. The Java mode applies to both secure and unsecure web connections.

Format	`no ip http java`
Mode	Privileged EXEC

ip http port

This command configures the TCP port number on which the HTP server listens for requests.

Default	80
Format	`ip http port` *`1-65535`*
Mode	Privileged EXEC

no ip http port

This command restores the HTTP server listen port to its factory default value.

Format	`no ip http port`
Mode	Privileged EXEC

ip http rest-api port

This command configures the HTTP TCP port number on which the open RESTful API server listens for RESTful requests.

Default	8080
Format	`ip http rest-api port` *`1025-65535`*
Mode	Privileged EXEC

no ip http rest-api port

This command restores the open RESTful API HTTP server listen port to its factory default value.

Format	`no ip http rest-api port`
Mode	Privileged EXEC

ip http rest-api secure-port

This command configures the HTTPS TCP port number on which the open RESTful API server listens for secure RESTful requests.

Default	8443
Format	`ip http rest-api secure-port` *`1025-65535`*
Mode	Privileged EXEC

no ip http rest-api secure-port

This command restores the open RESTful API HTTP server listen port to its factory default value.

Format	`no ip http rest-api secure-port`
Mode	Privileged EXEC

ip http session hard-timeout

This command configures the hard timeout for unsecure 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 reauthenticate. This timer begins on initiation of the web session and is unaffected by the activity level of the connection.

Default	24
Format	`ip http session hard-timeout` *`1-168`*
Mode	Privileged EXEC

no ip http session hard-timeout

This command restores the hard timeout for unsecure HTTP sessions to the default value.

Format	`no ip http session hard-timeout`
Mode	Privileged EXEC

ip http session maxsessions

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

Default	16
Format	`ip http session maxsessions` *`0-16`*
Mode	Privileged EXEC

no ip http session maxsessions

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

Format	`no ip http session maxsessions`
Mode	Privileged EXEC

ip http session soft-timeout

This command configures the soft timeout for unsecure 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 reauthenticate. This timer begins on initiation of the web session and is restarted with each access to the switch.

Default	5
Format	`ip http session soft-timeout` *`1-60`*
Mode	Privileged EXEC

no ip http session soft-timeout

This command resets the soft timeout for unsecure HTTP sessions to the default value.

Format	`no ip http session soft-timeout`
Mode	Privileged EXEC

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 reauthenticate. This timer begins on initiation of the web session and is

unaffected by the activity level of the connection. The secure-session hard-timeout cannot be set to zero (infinite).

Default	24
Format	`ip http secure-session hard-timeout` *`1-168`*
Mode	Privileged EXEC

no ip http secure-session hard-timeout

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

Format	`no ip http secure-session hard-timeout`
Mode	Privileged EXEC

ip http secure-session maxsessions

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

Default	16
Format	`ip http secure-session maxsessions` *`0-16`*
Mode	Privileged EXEC

no ip http secure-session maxsessions

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

Format	`no ip http secure-session maxsessions`
Mode	Privileged EXEC

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, the user is forced to reauthenticate. This timer begins on initiation of the web session and is restarted with each access to the switch. The secure-session soft-timeout can not be set to zero (infinite).

Default	5
Format	`ip http secure-session soft-timeout` *`1-60`*
Mode	Privileged EXEC

no ip http secure-session soft-timeout

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

Format	`no ip http secure-session soft-timeout`
Mode	Privileged EXEC

ip http secure-port

This command sets the SSL port, where port can be 1025-65535 and the default is 443.

Default	443
Format	`ip http secure-port` *`portid`*
Mode	Privileged EXEC

no ip http secure-port

This command resets the SSL port to the default value.

Format	`no ip http secure-port`
Mode	Privileged EXEC

ip http secure-protocol

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

Default	SSL3 and TLS1
Format	`ip http secure-protocol` *`[SSL3] [TLS1]`*
Mode	Privileged EXEC

show ip http

This command displays the HTTP settings for the switch.

Format	`show ip http`
Mode	Privileged EXEC

Column	Meaning
HTTP Mode (Unsecure)	The unsecure HTTP server administrative mode.
Java Mode	The java applet administrative mode which applies to both secure and unsecure web connections.
HTTP Port	The configured TCP port on which the HTTP server listens for requests. (The default is 80.)

Column	Meaning
RESTful API HTTP Port	The HTTPS TCP port number on which the OpEN RESTful API server listens for RESTful requests.
RESTful API HTTPS Port	The HTTPS TCP port number on which the OpEN RESTful API server listens for secure RESTful requests.
Maximum Allowable HTTP Sessions	The number of allowable unsecure HTTP sessions.
HTTP Session Hard Timeout	The hard timeout for unsecure HTTP sessions in hours.
HTTP Session Soft Timeout	The soft timeout for unsecure 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, TSL1, or both SSL3 and TSL1.
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 sessions in minutes.
Certificate Present	Whether the secure-server certificate files are present on the device.
Certificate Generation in Progress	Whether certificate generation is currently in progress.

Access Commands

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

disconnect

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

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

linuxsh

Use the `linuxsh` command to access the Linux shell. Use the `exit` command to exit the Linux shell and return to the 200 Series CLI. The shell session will timeout after five minutes of inactivity. The inactivity timeout value can be changed using the `session-timeout` command in Line Console mode (see session-timeout on page 48).

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

Parameter	Description
`ip-port`	The IP port number on which the Telnet daemon listens for connections. The range is 1 to 65535. The default value is 2324.

show loginsession

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

Format	`show loginsession`
Mode	Privileged EXEC

Column	Meaning
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 HTTP, HTTPS, Telnet, serial, or SSH.

show loginsession long

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

Format	`show loginsession long`
Mode	Privileged EXEC

The following shows an example of the command:

```
(Extreme 220) #show loginsession long
User Name
------------
```

```
admin
test1111test1111test1111test1111test1111test1111test1111test1111
```

User Account Commands

This section describes the commands used to add, manage, and delete system users. 200 Series software has two default users: admin and guest. The admin user can view and configure system settings, and the guest user can view settings.

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

aaa authentication login

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

The additional methods of authentication are used only if the previous method returns an error, not if there is an authentication failure. To ensure that the authentication succeeds even if all methods return an error, specify none as the final method in the command line. For example, if none is specified as an authentication method after radius, no authentication is used if the *RADIUS* server is down.

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

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

The following shows an example of the command:

```
(Extreme 220) (Config) # aaa authentication login default radius local enable none
```

no aaa authentication login

This command returns authentication login to the default.

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

aaa authentication enable

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

A separate default enable list, enableNetList, is used for Telnet and SSH users instead of enableList. This list is applied by default for Telnet and SSH, and contains enable followed by deny methods. In 200 Series, 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 enters the Privileged EXEC mode without entering the enable password.

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

The user manager returns ERROR (not PASS or FAIL) for enable and line methods if no password is configured, and moves to the next configured method in the authentication list. The method none reflects that there is no authentication needed.

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

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

See the following examples:

```
1 aaa authentication enable default enable none
2 aaa authentication enable default line none
3 aaa authentication enable default enable radius none
4 aaa authentication enable default line tacacs none
```

Examples 1 and 2 do not prompt for a password, however because examples 3 and 4 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, you are not prompted for a username – only for a password. 200 Series supports configuring methods after the

local method in authentication and authorization lists. If the user is not present in the local database, then the next configured method is tried.

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

Use the command show authorization methods on page 69 to display information about the authentication methods.

Note

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

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

Parameter	Description
default	Uses the listed authentication methods that follow this argument as the default list of methods, when using higher privilege levels.
list-name	Character string used to name the list of authentication methods activated, when using access higher privilege levels. Range: 1-15 characters.
method1 [method2...]	Specify at least one from the following: • **deny**: Used to deny access. • **enable**: Uses the enable password for authentication. • **line**: Uses the line password for authentication. • **none**: Uses no authentication. • **radius**: Uses the list of all RADIUS servers for authentication. • **tacacs**: Uses the list of all TACACS+ servers for authentication.

The following example sets authentication when accessing higher privilege levels:

```
(Extreme 220) (Config)# aaa authentication enable default enable
```

no aaa authentication enable

Use this command to return to the default configuration.

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

aaa authorization

Use this command to configure command and exec 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.

Note

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.

Per-Command Authorization

When authorization is configured for a line mode, the user manager sends information about an entered command to the AAA server. The AAA server validates the received command, and responds with either a PASS or FAIL response. If approved, the command is executed. Otherwise, the command is denied and an error message is shown to the user. The various utility commands like tftp, and ping, and outbound Telnet should also pass command authorization. Applying the script is treated as a single command apply script, which also goes through authorization. Startup-config commands applied on device boot-up are not an object of the authorization process.

The per-command authorization usage scenario is this:

1 Configure Authorization Method List:

```
aaa authorization commands listname tacacs radius none
```

2 Apply AML to an Access Line Mode (console, Telnet, SSH):

```
authorization commands listname
```

3 Commands entered by the user will go through command authorization via TACACS+ or RADIUS server and will be accepted or denied.

```
Exec Authorization
```

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

The exec authorization usage scenario is this:

1 Configure Authorization Method List:

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

2 Apply AML to an Access Line Mode (console, Telnet, SSH):

```
authorization exec listname
```

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

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

Parameter	Description
`commands`	Provides authorization for all user-executed commands.
`exec`	Provides exec authorization.
`default`	The default list of methods for authorization services.
`list-name`	Alphanumeric character string used to name the list of authorization methods.
`method`	**`TACACS+/RADIUS/Local`** and **`none`** are supported.

The following shows an example of the command:

```
(Extreme 220) (Routing) #
(Extreme 220) (Routing) #configure
(Extreme 220) (Config) (Config)#aaa authorization exec default  tacacs+ none
(Extreme 220) (Config) (Config)#aaa authorization commands default tacacs+ none
```

no aaa authorization

This command deletes the authorization method list.

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

authorization commands

This command applies a command authorization method list to an access method (console, telnet, ssh). For usage scenarios on per command authorization, see the command aaa authorization on page 67.

Format	`authorization commands [default|`*`list-name`*`]`
Mode	Line console, Line telnet, Line SSH

Parameter	Description
`commands`	This causes command authorization for each command execution attempt.

The following shows an example of the command:

```
(Extreme 220) (Config) #line console
(Extreme 220) (Config-line)#authorization commands list2
(Extreme 220) (Config-line)#exit
```

no authorization commands

This command removes command authorization from a line config mode.

Format	`no authorization {commands|exec}`
Mode	Line console, Line telnet, Line SSH

authorization exec

This command applies a command authorization method list to an access method so that the user may not be required to use the `enable` command to enter Privileged EXEC mode. For usage scenarios on exec authorization, see the command aaa authorization on page 67.

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

Parameter	Description
`list-name`	The command authorization method list.

no authorization exec

This command removes command authorization from a line config mode.

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

authorization exec default

This command applies a default command authorization method list to an access method so that the user may not be required to use the `enable` command to enter Privileged EXEC mode. For usage scenarios on exec authorization, see the command aaa authorization on page 67.

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

no authorization exec default

This command removes command authorization from a line config mode.

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

show authorization methods

This command displays the configured authorization method lists.

Format	`show authorization methods`
Mode	Privileged EXEC

The following example shows CLI display output for the command.

```
(Extreme 220) #show authorization methods
Command Authorization List                                          Method
-------------------------- ---------------------------------------
dfltCmdAuthList                          tacacs         none
list2                                 none          undefined
list4                                   tacacs         undefined
Line                  Command Method List
------------ ------------------------------
Console                  dfltCmdAuthList
Telnet                   dfltCmdAuthList
SSH                      dfltCmdAuthList
Exec Authorization Method List
-----------------------   ---------------------------------------
dfltExecAuthList                         tacacs         none
list2                                 none          undefined
list4                                 tacacs        undefined
Line                      Exec Method List
------------ ------------------------------
Console                   dfltExecAuthList
Telnet                    dfltExecAuthList
SSH                       dfltExecAuthList
```

enable authentication

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

Format	`enable authentication {default | list-name}`
Mode	Line Config

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

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

```
(Extreme 220) (Config)# line console
(Extreme 220)(config-line)# enable authentication default
```

no enable authentication

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

Format	`no enable authentication`
Mode	Line Config

username (Global Config)

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

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

Parameter	Description
`name`	The name of the user. Range is 1-64 characters.
`password`	The authentication password for the user. Range is 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 is 0-15. Enter access level 1 for non-privileged (switch> prompt) or 15 for highest privilege (switch# prompt) Access. If not specified where it is optional, the privilege level is 1.
`encrypted`	Encrypted password entered, copied from another switch configuration.
`override-complexity-check`	Disables the validation of the password strength.

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

```
(Extreme 220) (Config)# username bob password xxxyyymmmm level 15
```

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

```
(Extreme 220) (Config) # username test password testPassword level 1 override-complexity-check
```

The following example configures user 'test' with password 'testtest'. No level is assigned.

```
(Extreme 220) (Config) #username test password testtest
```

The following example configures user 'test' with a complex password and a user level of 1. The password is encrypted. The level is then increased to 15 and a new password created.

```
(Extreme 220) (Config) # username test password
e8d63677741431114f9e39a853a15e8fd35ad059e2e1b49816c243d7e08152b052eafbf23b528d348cdba1b1b7a
b91be842278e5e970dbfc62d16dcd13c0b864 level 1 encrypted override-complexity-check
(Extreme 220) (Config) #  username test level 15 password
```

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

The following example changes the password for user 'test'.

```
(Extreme 220) (Config) # username test level 15 override-complexity-check  password
Enter new password:********
Confirm new password:********
```

no username

Use this command to remove a user name.

Format	`no username name`
Mode	Global Config

username nopassword

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

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

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

username unlock

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

Format	`username name unlock`
Mode	Global Config

username snmpv3 accessmode

This command specifies the SNMPv3 access privileges for the specified login user. The valid accessmode values are readonly or readwrite. The username is the login user name for which the

specified access mode applies. The default is readwrite for the “admin” user and readonly for all other users.

Note
You must enter the username in the same case you used when you added the user. To see the case of the username, enter the `show users` command.

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

no username snmpv3 accessmode

This command sets the SNMPv3 access privileges for the specified user as readwrite for the “admin” user and readonly for all other users. The username value is the user name for which the specified access mode will apply.

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

username snmpv3 authentication

This command specifies the authentication protocol to be used for the specified user. The valid authentication protocols are none, md5 or sha. If you specify md5 or sha, the login password is also used as the SNMPv3 authentication password and therefore must be at least eight characters in length. The username is the user name associated with the authentication protocol.

Note
You must enter the username in the same case you used when you added the user. To see the case of the username, enter the `show users` command.

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

no username snmpv3 authentication

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

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

username snmpv3 encryption

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

If you select des, you can specify the required key in the command line. The encryption key must be 8 to 64 characters long. If you select the des protocol but do not provide a key, the user is prompted for the key. When you use the des protocol, the login password is also used as the SNMPv3 encryption password, so it must be a minimum of eight characters. If you select none, you do not need to provide a key.

The username value is the login user name associated with the specified encryption.

Note
You must enter the username in the same case you used when you added the user. To see the case of the username, enter the `show users` command.

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

no username snmpv3 encryption

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

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

username snmpv3 encryption encrypted

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

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

show users

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

Format	`show users`
Mode	Privileged EXEC

Column	Meaning
User Name	The name the user enters to login using the serial port, Telnet or web.
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.
SNMPv3 Access Mode	The SNMPv3 Access Mode. If the value is set to ReadWrite, the SNMPv3 user is able to set and retrieve parameters on the system. If the value is set to ReadOnly, the SNMPv3 user is only able to retrieve parameter information. The SNMPv3 access mode may be different than the CLI and web access mode.
SNMPv3 Authentication	The authentication protocol to be used for the specified login user.
SNMPv3 Encryption	The encryption protocol to be used for the specified login user.

show users long

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

Format	`show users long`
Mode	Privileged EXEC

The following shows an example of the command.

```
(Extreme 220) #show users long
User Name
------------
admin
guest
test1111test1111test1111test1111
```

show users accounts

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

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

Column	Meaning
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.

Column	Meaning
Password Expiry Date	The current password expiration date in date format.
Lockout	Whether the user account is locked out (true or false).

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

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

The following example displays information about the local user database.

```
(Extreme 220) #show users accounts
UserName            Privilege Password Password     Lockout
                              Aging    Expiry date
------------------- --------- -------- ------------ -------
admin               15        ---      ---          False
guest               1         ---      ---          False
console#show users accounts detail
UserName..................................... admin
Privilege.................................... 15
Password Aging............................... ---
Password Expiry.............................. ---
Lockout...................................... False
Override Complexity Check.................... Disable
Password Strength............................ ---
UserName..................................... guest
Privilege.................................... 1
Password Aging............................... ---
Password Expiry.............................. ---
Lockout...................................... False
Override Complexity Check.................... Disable
Password Strength............................ ---
```

show users login-history [long]

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

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

show users login-history [username]

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

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

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

The following example shows user login history outputs.

```
Console>show users login-history
Login Time            Username  Protocol  Location
--------------------  --------- --------- ---------------
Jan 19 2005 08:23:48  Bob       Serial
Jan 19 2005 08:29:29  Robert    HTTP      172.16.0.8
Jan 19 2005 08:42:31  John      SSH       172.16.0.1
Jan 19 2005 08:49:52  Betty     Telnet    172.16.1.7
```

login authentication

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

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

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

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

```
(Extreme 220) (Config) # line console
(Extreme 220) (config-line)# login authentication default
```

no login authentication

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

password

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

Format	`password`
Mode	User EXEC

The following is an example of the command.

```
console>password
Enter old password:********
Enter new password:********
Confirm new password:********
```

password (Line Configuration)

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

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

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

The following examples show three different ways of using the command.

```
(Extreme 220)(Config-line)# password testtest
(Extreme 220) (Config-line)# password
e8d63677741431114f9e39a853a15e8fd35ad059e2e1b49816c243d7e08152b052eafbf23b528d348cdba1b1b7a
b91be842278e5e970dbfc62d16dcd13c0b864 encrypted
(Extreme 220) (Config-line)# password
Enter new password:********
Confirm new password:********
```

no password (Line Configuration)

Use this command to remove the password on a line.

Format	`no password`
Mode	Line Config

password (User EXEC)

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

Format	`password`
Mode	User EXEC

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

```
(Extreme 220)>password
Enter old password:********
Enter new password:********
Confirm new password:********
```

password (aaa IAS User Config)

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

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

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

```
(Extreme 220) #
(Extreme 220) #configure
(Extreme 220) (Config) #aaa ias-user username 1f3ccb1157
(Extreme 220) (Config-aaa-ias-User)#password 1f3ccb1157
(Extreme 220) (Config-aaa-ias-User)#exit
(Extreme 220) (Config) #
```

no password (aaa IAS User Config)

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

Format	no password
Mode	aaa IAS User Config

The following shows an example of the command.

```
(Extreme 220) #
(Extreme 220) #configure
(Extreme 220) (Config) #aaa ias-user username client-1
(Extreme 220) (Config-aaa-ias-User)#password client123
(Extreme 220) (Config-aaa-ias-User)#no password
```

enable password (Privileged EXEC)

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

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

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

The following shows an example of the command.

```
(Extreme 220) #enable password testtest
(Extreme 220) #enable password
e8d63677741431114f9e39a853a15e8fd35ad059e2e1b49816c243d7e08152b052eafbf23b528d348cdba1b1b7a
b91be842278e5e970dbfc62d16dcd13c0b864 encrypted
```

```
(Extreme 220) #enable password
Enter old password:********
Enter new password:********
Confirm new password:********
```

no enable password (Privileged EXEC)

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

Format	`no enable password`
Mode	Privileged EXEC

passwords min-length

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

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

no passwords min-length

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

Format	`no passwords min-length`
Mode	Global Config

passwords history

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

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

no passwords history

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

Format	`no passwords history`
Mode	Global Config

passwords aging

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

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

no passwords aging

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

Format	`no passwords aging`
Mode	Global Config

passwords lock-out

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

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

no passwords lock-out

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

Format	`no passwords lock-out`
Mode	Global Config

passwords strength-check

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

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

no passwords strength-check

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

Format	`no passwords strength-check`
Mode	Global Config

passwords strength maximum consecutive-characters

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

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

passwords strength maximum repeated-characters

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

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

passwords strength minimum uppercase-letters

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

Default	2
Format	`passwords strength minimum uppercase-letters` *`0-16`*
Mode	Global Config

no passwords strength minimum uppercase-letters

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

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

passwords strength minimum lowercase-letters

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

Default	2
Format	`passwords strength minimum lowercase-letters` *`0-16`*
Mode	Global Config

no passwords strength minimum lowercase-letters

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

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

passwords strength minimum numeric-characters

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

Default	2
Format	`passwords strength minimum numeric-characters` *`0-16`*
Mode	Global Config

no passwords strength minimum numeric-characters

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

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

passwords strength minimum special-characters

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

Default	2
Format	`passwords strength minimum special-characters` *`0-16`*
Mode	Global Config

no passwords strength minimum special-characters

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

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

passwords strength minimum character-classes

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

Default	4
Format	`passwords strength minimum character-classes` *`0-4`*
Mode	Global Config

no passwords strength minimum character-classes

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

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

passwords strength exclude-keyword

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

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

no passwords strength exclude-keyword

Use this command to reset the restriction for a specific keyword or for all keywords.

The **keyword** parameter is optional. If you issue the command with no keywords, then no keywords will be restricted.

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

show passwords configuration

Use this command to display the configured password management settings.

Format	`show passwords configuration`
Mode	Privileged EXEC

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

show passwords result

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

Format	`show passwords result`
Mode	Privileged EXEC

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

aaa ias-user username

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

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

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

no aaa ias-user username

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

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

The following shows an example of the command.

```
(Extreme 220) #
(Extreme 220) #configure
(Extreme 220) (Config) #aaa ias-user username client-1
(Extreme 220) (Config-aaa-ias-User)#exit
(Extreme 220) (Config)#no aaa ias-user username client-1
(Extreme 220) (Config) #
```

aaa session-id

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

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

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

no aaa session-id

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

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

aaa accounting

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

Note

- A maximum of five Accounting Method lists can be created for each exec and commands type.
- Only the default Accounting Method list can be created for DOT1X. There is no provision to create more.
- The same list-name can be used for both exec and commands accounting type
- AAA Accounting for commands with RADIUS as the accounting method is not supported.
- Start-stop or None are the only supported record types for DOT1X accounting. Start-stop enables accounting and None disables accounting.
- RADIUS is the only accounting method type supported for DOT1X accounting.

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

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

The following shows an example of the command.

```
(Extreme 220) (Routing) #
(Extreme 220) (Routing) #configure
(Extreme 220) (Routing) #aaa accounting commands default stop-only tacacs
(Extreme 220) (Routing) #aaa accounting exec default start-stop radius
(Extreme 220) (Routing) #aaa accounting dot1x default start-stop radius
(Extreme 220) (Routing) #aaa accounting dot1x default none
(Extreme 220) (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 to first delete the previous configuration.

```
(Extreme 220) (Routing) #
(Extreme 220) (Routing) #configure
(Extreme 220) (Routing) #aaa accounting exec ExecList stop-only tacacs
(Extreme 220) (Routing) #aaa accounting exec ExecList start-stop tacacs
(Extreme 220) (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 the record type to start-stop from stop-only for the same method list. The third command, for the same list changes the methods list to {tacacs,radius} from {tacacs}.

no aaa accounting

This command deletes the accounting method list.

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

The following shows an example of the command.

```
(Extreme 220) (Routing) #
(Extreme 220) (Routing) #configure
(Extreme 220) (Routing) #aaa accounting commands userCmdAudit stop-only tacacs radius
(Extreme 220) (Routing) #no aaa accounting commands userCmdAudit
(Extreme 220) (Routing) #exit
```

password (AAA IAS User Configuration)

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

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

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

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

```
(Extreme 220) #
(Extreme 220) #configure
(Extreme 220) (Config) #aaa ias-user username 1f3ccb1157
(Extreme 220) (Config-aaa-ias-User)#password 1f3ccb1157
(Extreme 220) (Config-aaa-ias-User)#exit
(Extreme 220) (Config) #
```

no password (AAA IAS User Configuration)

Use this command to clear a user's password.

Format	`no password`
Mode	AAA IAS User Config

The following shows an example of the command.

```
(Extreme 220) #
(Extreme 220) #configure
(Extreme 220) (Config) #aaa ias-user username client-1
(Extreme 220) (Config-aaa-ias-User)#password client123
(Extreme 220) (Config-aaa-ias-User)#no password
```

clear aaa ias-users

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

Format	`clear aaa ias-users`
Mode	Privileged EXEC

show aaa ias-users

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

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

The following is an example of the command.

```
(Extreme 220) (Routing) #
(Extreme 220) (Routing) #show aaa ias-users
UserName
------------------
Client-1
Client-2
```

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

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

accounting

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

Format	`accounting {exec | commands} {default | list_name}`
Mode	Line Configuration

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

The following is a example of the command.

```
(Extreme 220) (Routing) #
(Extreme 220) (Routing) #configure
(Extreme 220) (Config) #line telnet
(Extreme 220) (Routing)(Config-line)# accounting exec default
(Extreme 220) (Routing) #exit
```

no accounting

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

Format	`no accounting {exec|commands}`
Mode	Line Configuration

show accounting

Use this command to display ordered methods for accounting lists.

Format	`show accounting`
Mode	Privileged EXEC

The following example shows CLI display output for the command.

```
(Extreme 220) (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
```

show accounting methods

Use this command to display configured accounting method lists.

Format	`show accounting methods`
Mode	Privileged EXEC

The following example shows CLI display output for the command.

```
(Extreme 220) (Routing) #
(Extreme 220) (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
```

clear accounting statistics

This command clears the accounting statistics.

Format	`clear accounting statistics`
Mode	Privileged EXEC

show domain-name

This command displays the configured domain-name.

Format	`show domain-name`
Mode	Privileged EXEC

The following example shows CLI display output for the command.

```
(Extreme 220) (Routing) #
(Extreme 220) (Routing) #show domain-name
Domain                : Enable
Domain-name           :abc
```

SNMP Commands

This section describes the commands used to configure *SNMP* on the switch. You can configure the switch to act as an SNMP agent so that it can communicate with SNMP managers on your network.

snmp-server

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

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

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

snmp-server community

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

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

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

Parameter	Description
`community-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-name`** can be up to 16 case-sensitive characters.
`ro | rw | su`	The access mode of the SNMP community, which can be public (Read-Only/RO), private (Read-Write/RW), or Super User (SU).

Parameter	Description
ip-address	The associated community SNMP packet sending address and is used along with the client IP mask value to denote a range of IP addresses from which SNMP clients may use that community to access the device. A value of 0.0.0.0 allows access from any IP address. Otherwise, this value is ANDed with the mask to determine the range of allowed client IP addresses.
view-name	The name of the view to create or update.

no snmp-server community

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

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

snmp-server community-group

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

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

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

snmp-server enable traps violation

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

Note
For other port security commands, see Port Security Commands on page 454.

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

no snmp-server enable traps violation

This command disables the sending of new violation traps.

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

snmp-server enable traps

This command enables the Authentication Flag.

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

no snmp-server enable traps

This command disables the Authentication Flag.

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

snmp-server enable traps bgp

The **bgp** option on the `snmp-server enable traps` command (see snmp-server enable traps on page 94) enables the two traps defined in the standard BGP MIB, RFC 4273. A trap is sent when an adjacency reaches the ESTABLISHED state and when a backward adjacency state transition occurs.

Default	BGP traps are disabled by default.
Format	`snmp-server enable traps bgp state-changes limited`
Mode	Global Config

Parameter	Description
state-changes limited	Enable standard traps defined in RFC 4273.

no snmp-server enable traps bgp state-changes limited

This command disables the two traps defined in the standard BGP MIB, RFC 4273.

Format	`no snmp-server enable traps bgp state-changes limited`
Mode	Global Config

snmp-server enable traps fip-snooping

Note
This command may not be available on all platforms.

This command enables FCoE Initialization Protocol (FIP) snooping traps for the entire switch. When enabled, link traps are sent only if the Link Trap flag setting associated with the port is enabled. show snmp on page 104

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

no snmp-server enable traps fip-snooping

Note
This command may not be available on all platforms.
This command disables FCoE Initialization Protocol (FIP) snooping traps for the entire switch.

Default	enabled
Format	`no snmp-server enable traps fip-snooping`
Mode	Global Config

snmp-server port

This command configures the UDP port number on which the *SNMP* server listens for requests.

Default	161
Format	`snmp-server port` *`1025-65535`*
Mode	Privileged EXEC

no snmp-server port

This command restores the *SNMP* server listen port to its factory default value.

Format	no snmp-server port
Mode	Privileged EXEC

snmp trap link-status

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

Note
This command is valid only when the Link Up/Down Flag is enabled. no snmp-server enable traps bgp state-changes limited on page 95

Format	snmp trap link-status
Mode	Interface Config

no snmp trap link-status

This command disables link status traps by interface.

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

Format	no snmp trap link-status
Mode	Interface Config

snmp trap link-status all

This command enables link status traps for all interfaces.

Note
This command is valid only when the Link Up/Down Flag is enabled. See snmp-server enable traps bgp on page 94.

Format	snmp trap link-status all
Mode	Global Config

no snmp trap link-status all

This command disables link status traps for all interfaces.

Note
This command is valid only when the Link Up/Down Flag is enabled. See snmp-server enable traps bgp on page 94.

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

snmp-server enable traps linkmode

This command enables Link Up/Down traps for the entire switch. When enabled, link traps are sent only if the Link Trap flag setting associated with the port is enabled. show snmp on page 104

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

no snmp-server enable traps linkmode

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

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

snmp-server enable traps multiusers

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

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

no snmp-server enable traps multiusers

This command disables Multiple User traps.

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

snmp-server enable traps stpmode

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

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

no snmp-server enable traps stpmode

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

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

snmp-server engineID local

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

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

Parameter	Description
`engineid-string`	A hexadecimal string identifying the engine ID, used for localizing configuration. Engine ID must be an even length in the range of 6 to 32 hexadecimal characters.
`default`	Sets the engine ID to the default string, based on the device MAC address.

Caution
Changing the engine ID will invalidate all SNMP configuration that exists on the box.

no snmp-server engineID local

This command removes the specified engine ID.

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

snmp-server filter

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

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

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

no snmp-server filter

This command removes the specified filter.

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

snmp-server group

This command creates an *SNMP* access group.

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

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

Parameter	Description
priv	This group can be accessed only when using both Authentication and Encryption. Applicable only if SNMPv3 is selected.
context-name	The SNMPv3 context used during access. Applicable only if SNMPv3 is selected.
read-view	The view this group will use during GET requests. The range is 1 to 30 characters.
write-view	The view this group will use during SET requests. The range is 1 to 30 characters.
notify-view	The view this group will use when sending out traps. The range is 1 to 30 characters.

no snmp-server group

This command removes the specified group.

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

snmp-server host

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

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

Parameter	Description
host-addr	The IPv4 or IPv6 address of the host to send the trap or inform to.
traps	Send *SNMP* traps to the host. This option is selected by default.
version 1	Sends SNMPv1 traps. This option is not available if informs is selected.
version 2	Sends SNMPv2c traps. This option is not available if informs is selected. This option is selected by default.
informs	Send SNMPv2 informs to the host.
seconds	The number of seconds to wait for an 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.
community-string	Community string sent as part of the notification. The range is 1 to 20 characters.

Parameter	Description
port	The SNMP Trap receiver port. The default is port 162.
filter-name	The filter name to associate with this host. Filters can be used to specify which traps are sent to this host. The range is 1 to 30 characters.

no snmp-server host

This command removes the specified host entry.

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

snmp-server user

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

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

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

no snmp-server user

This command removes the specified SNMPv3 user.

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

snmp-server view

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

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

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

no snmp-server view

This command removes the specified view.

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

snmp-server v3-host

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

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

Parameter	Description
host-addr	The IPv4 or IPv6 address of the host to send the trap or inform to.
user-name	User who sends a Trap or Inform message. This user must be associated with a group that supports the version and access method. The range is 1 to 30 characters.
traps	Send *SNMP* traps to the host. This is the default option.
informs	Send SNMP informs to the host.
seconds	Number of seconds to wait for an acknowledgement before resending the Inform. The default is 15 seconds. The range is 1 to 300 seconds.

Parameter	Description
retries	Number of times to resend an Inform. The default is 3 attempts. The range is 0 to 255 retries.
auth	Enables authentication but not encryption.
noauth	No authentication or encryption. This is the default.
priv	Enables authentication and encryption.
port	The SNMP Trap receiver port. This value defaults to port 162.
filter-name	The filter name to associate with this host. Filters can be used to specify which traps are sent to this host. The range is 1 to 30 characters.

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.

Format	`snmptrap source-interface {unit/slot/port | loopback loopback-id|tunnel tunnel-id|vlan vlan-id}`
Mode	Global Configuration

Parameter	Description
unit/slot/port	The unit identifier assigned to the switch.
loopback-id	Configures the loopback interface. The range of the loopback ID is 0 to 7.
tunnel-id	Configures the IPv6 tunnel interface. The range of the tunnel ID is 0 to 7.
vlan-id	Configures the VLAN interface to use as the source IP address. The range of the VLAN ID is 1 to 4093.

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.

Format	`no snmptrap source-interface`
Mode	Global Configuration

snmptrap ipaddr snmpversion

This command modifies the *SNMP* version of a trap. The maximum length of name is 16 case-sensitive alphanumeric characters. The *snmpversion* options are snmpv1 or snmpv2.

Note
This command does not support a “no” form.

Format	`snmptrap ipaddr snmpversion` *`name snmpversion`*
Mode	Global Configuration

snmptrap ip6addr snmpversion

This command modifies the *SNMP* version of a trap. The maximum length of name is 16 case-sensitive alphanumeric characters. The *`snmpversion`* options are snmpv1 or snmpv2.

Note
This command does not support a “no” form.

Format	`snmptrap ip6addr snmpversion` *`name snmpversion`*
Mode	Global Configuration

show snmp

This command displays the current *SNMP* configuration.

Format	`show snmp`
Mode	Privileged EXEC

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

Column	Meaning
Filter name	The filter the traps will be limited by for this host.
TO Sec	The number of seconds before informs will time out when sending to this host.
Retries	The number of times informs will be sent after timing out.

show snmp engineID

This command displays the currently configured *SNMP* engineID.

Format	`show snmp engineID`
Mode	Privileged EXEC

Column	Meaning
Local SNMP engineID	The current configuration of the displayed SNMP engineID.

show snmp filters

This command displays the configured filters used when sending traps.

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

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

show snmp group

This command displays the configured groups.

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

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

show snmp-server

This command displays the current *SNMP* server user configuration.

Format	`show snmp-server`
Mode	Privileged EXEC

The following example shows CLI display output for the command.

```
(Extreme 220)#show snmp-server
SNMP Server Port.............................. 161
```

show snmp source-interface

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

Format	`show snmp source-interface`
Mode	Privileged EXEC

The following example shows CLI display output for the command.

```
(Extreme 220) (Routing)# show snmp source-interface
SNMP trap Client Source Interface.............. (not configured)
```

show snmp user

This command displays the currently configured SNMPv3 users.

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

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

show snmp views

This command displays the currently configured views.

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

Column	Meaning
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.

show trapflags

This command displays trap conditions. The command's display shows all the enabled OSPFv2 and *OSPFv3 (Open Shortest Path First version 3)* trapflags. Configure which traps the switch should generate by enabling or disabling the trap condition. If a trap condition is enabled and the condition is detected, the *SNMP* agent on the switch sends the trap to all enabled trap receivers. You do not have to reboot the switch to implement the changes. Cold and warm start traps are always generated and cannot be disabled.

Format	`show trapflags`
Mode	Privileged EXEC

Column	Meaning
Authentication Flag	Can be enabled or disabled. The factory default is enabled. Whether authentication failure traps will be sent.
Link Up/Down Flag	Can be enabled or disabled. The factory default is enabled. Whether link status traps will be sent.
Multiple Users Flag	Can be enabled or disabled. The factory default is enabled. 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. Whether spanning tree traps are sent.
ACL Traps	May be enabled or disabled. The factory default is disabled. Whether ACL traps are sent.
BGP4 Traps	Can be enabled or disabled. The factory default is disabled. Whether BGP4 traps are sent. (This field appears only on systems with the BGPv4 software package installed.)
DVMRP Traps	Can be enabled or disabled. The factory default is disabled. Whether DVMRP traps are sent.
OSPFv2 Traps	Can be enabled or disabled. The factory default is disabled. 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.
OSPFv3 Traps	Can be enabled or disabled. The factory default is disabled. Whether OSPF traps are sent. If any of the OSPFv3 trap flags are not enabled, then the command displays *`disabled`*. Otherwise, the command shows all the enabled OSPFv3 traps' information.
PIM Traps	Can be enabled or disabled. The factory default is disabled. Whether PIM traps are sent.

RADIUS Commands

This section describes the commands used to configure the switch to use a *RADIUS* server on your network for authentication and accounting.

aaa server radius dynamic-author

This command enables CoA functionality and enters dynamic authorization local server configuration mode.

Default	None
Format	`aaa server radius dynamic-author`
Mode	Global Config

```
(Extreme 220) (Routing) #configure
(Extreme 220) (Config) (Config)#aaa server radius dynamic-author
(Extreme 220) (Config- radius-da)#
```

no aaa server radius dynamic-author

This command disables CoA functionality.

Default	None
Format	`no aaa server radius dynamic-author`
Mode	Global Config

```
(Extreme 220) #configure
(Extreme 220) (Config) #no aaa server radius dynamic-author
```

auth-type

Use this command to specify the type of authorization that the device uses for *RADIUS* clients. The client must match the configured attributes for authorization.

Default	All
Format	`auth-type {any | all | session-key}`
Mode	Dynamic Authorization

no auth-type

Use this command to reset the type of authorization that the device must use for *RADIUS* clients.

Default	None
Format	`no auth-type`
Mode	Dynamic Authorization

authorization network radius

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

Default	Disabled
Format	`authorization network radius`
Mode	Global Config

no authorization network radius

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

Format	`no authorization network radius`
Mode	Global Config

clear radius dynamic-author statistics

This command clears RADIUS dynamic authorization counters.

Default	None
Format	`clear radius dynamic-author statistics`
Mode	Privileged EXEC

```
 (Extreme 220) (Routing) #clear radius dynamic-author statistics
Are you sure you want to clear statistics? (y/n) y
Statistics cleared.
```

client

Use this command to configure the IP address or hostname of the AAA server client. Use the optional **`server-key`** keyword and string argument to configure the server key at the client level.

Default	None
Format	`client { ip-address | hostname } [server-key [0|7] key-string]`
Mode	Dynamic Authorization

```
(Extreme 220) (Config- radius-da)#client 10.0.0.1 server-key 7  device1
```

no client

Use this command to remove the configured Dynamic Authorization client and the key associated with that client in the device.

Default	None
Format	`no client { ip-address | hostname }`
Mode	Dynamic Authorization

```
(Extreme 220) (Config- radius-da)#no client 10.0.0.1
```

debug aaa coa

Use this command to display Dynamic Authorization Server processing debug information.

Default	None
Format	`debug aaa coa`
Mode	Dynamic Authorization

debug aaa pod

Use this command to display Disconnect Message packets.

Default	None
Format	`debug aaa pod`
Mode	Dynamic Authorization

ignore server-key

Use this optional command to configure the device to ignore the server key.

Default	Disabled
Format	`ignore server-key`
Mode	Dynamic Authorization

```
(Extreme 220) (Config- radius-da)#ignore server-key
```

no ignore server-key

Use this command to configure the device not to ignore the server key (that is, it resets the ignore server key property on the device).

Default	Disabled
Format	`no ignore server-key`
Mode	Dynamic Authorization

```
(Extreme 220) (Config- radius-da)#no ignore server-key
```

ignore session-key

Use this optional command to configure the device to ignore the session key.

Default	Disable
Format	`ignore session-key`
Mode	Dynamic Authorization

no ignore session-key

Use this command to configure the device to not ignore the session key (that is, it resets the ignore session key property on the device).

Default	Disabled
Format	`no ignore session-key`
Mode	Dynamic Authorization

port

Use this command to specify the UDP port on which a device listens for *RADIUS* requests from configured Dynamic Authorization clients. The supported range for *`port-number`* is 1025 to 65535.

Default	3799
Format	`port` *`port-number`*
Mode	Dynamic Authorization

```
(Extreme 220) (Config- radius-da)#port 1700
```

no port

Use this command to reset the configured UDP port on which a device listens for *RADIUS* requests from configured Dynamic Authorization clients.

Default	3799
Format	`no port`
Mode	Dynamic Authorization

```
(Extreme 220) (Config- radius-da)#no port
```

radius accounting mode

This command is used to enable the *RADIUS* accounting function.

Default	Disabled
Format	`radius accounting mode`
Mode	Global Config

no radius accounting mode

This command is used to set the *RADIUS* accounting function to the default value - that is, the RADIUS accounting function is disabled.

Format	`no radius accounting mode`
Mode	Global Config

radius server attribute 4

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

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

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

no radius server attribute 4

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

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

The following shows an example of the command.

```
(Extreme 220) (Config) #radius server attribute 4  192.168.37.60
(Extreme 220) (Config) #radius server attribute 4
```

radius server host

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

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

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

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

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

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

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

no radius server host

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

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

The following shows an example of the command.

```
(Extreme 220) (Config) #radius server host acct 192.168.37.60
(Extreme 220) (Config) #radius server host acct 192.168.37.60 port 1813
(Extreme 220) (Config) #radius server host auth 192.168.37.60 name Network1_RS port 1813
(Extreme 220) (Config) #radius server host acct 192.168.37.60 name Network2_RS
(Extreme 220) (Config) #no radius server host acct 192.168.37.60
```

radius server key

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

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

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

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

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

The following shows an example of this command, with *`encrypt-string`* representing the encrypted password.

```
radius server key acct 10.240.4.10 encrypted encrypt-string
```

radius server msgauth

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

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

Parameter	Description
ipaddr	The IP address of the server.
dnsname	The DNS name of the server.

no radius server msgauth

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

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

radius server primary

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

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

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

radius server retransmit

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

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

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

no radius server retransmit

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

Format	`no radius server retransmit`
Mode	Global Config

radius 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.

Format	`radius source-interface {`*`unit/slot/port`* `| loopback` *`loopback-id`* `|` **`vlan`** *`vlan-id`*`}`
Mode	Global Config

Parameter	Description
`unit/slot/port`	The unit identifier assigned to the switch.
`loopback-id`	Configures the loopback interface. The range of the loopback ID is 0 to 7.
`vlan-id`	Configures the VLAN interface to use as the source IP address. The range of the VLAN ID is 1 to 4093.

no radius source-interface

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

Format	`no radius source-interface`
Mode	Global Config

radius server timeout

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

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

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

no radius server timeout

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

Format	`no radius server timeout`
Mode	Global Config

server-key

Use this command to configure a global shared secret that is used for all dynamic authorization clients that do not have an individual shared secret key configured.

Default	None
Format	`server-key [` **`0`** `|` **`7`**`]` *`key-string`*
Mode	Dynamic Authorization

Parameter	Description
0	An unencrypted key is to be entered
7	An encrypted key is to be entered
`key-string`	The shared secret string. Maximum length is 128 characters for unencrypted key and 256 characters for encrypted key. Overrides the global setting for this client only. Enclose in quotes to use special characters or embedded blanks.

The following shows an example of this command:

```
(Extreme 220) (Config-radius-da)# server-key encrypted mydevice
```

no server-key

Use this command to remove the global shared secret key configuration.

Default	None
Format	`no server-key`
Mode	Dynamic Authorization

```
(Extreme 220) (Config-radius-da)#no server-key
```

show radius servers

Use this command to display the authentication parameters.

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

```
(Extreme 220)# show radius servers name Default-RADIUS-Server
RADIUS Server Name.............................. CoA-Server-1
Current Server IP Address....................... 1.1.1.1
Number of Retransmits........................... 3
Timeout Duration................................ 15
Deadtime........................................ 0
Port............................................ 3799
Source IP....................................... 10.27.9.99 <- switch
RADIUS Accounting Mode.......................... Disabled
Secret Configured............................... Yes
Message Authenticator........................... Enable
Number of CoA Requests Received..................... 203
Number of CoA ACK Responses Sent.................... 111
Number of CoA NAK Responses Sent..................... 37
Number of Coa Requests Ignored....................... 55
Number of CoA Missing/Unsupported Attribute Requests.....  18
Number of CoA Session Context Not Found Requests.........  5
Number of CoA Invalid Attribute Value Requests... 11
Number of Administratively Prohibited Requests.........3
```

show radius

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

Format	`show radius`
Mode	Privileged EXEC

Column	Meaning
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.

Column	Meaning
Number of Named Accounting Server Groups	The number of configured named RADIUS server groups.
Number of Retransmits	The configured value of the maximum number of times a request packet is retransmitted.
Time Duration	The configured timeout value, in seconds, for request retransmissions.
RADIUS Accounting Mode	A global parameter to indicate whether 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.

The following example shows CLI display output for the command.

```
(Extreme 220) #show radius
        Number of Configured Authentication Servers..... 32
        Number of Configured Accounting Servers......... 32
        Number of Named Authentication Server Groups..... 15
        Number of Named Accounting Server Groups........ 3
        Number of Retransmits........................... 4
        Time Duration................................... 10
        RADIUS Accounting Mode.......................... Disable
        RADIUS Attribute 4 Mode......................... Enable
        RADIUS Attribute 4 Value ....................... 192.168.37.60
```

show radius servers

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

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

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.

Column	Meaning
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.

Column	Meaning
Current Host Address	The IP address of the currently active authenticating server.
Secret Configured	Yes or No Boolean value that indicates whether this server is configured with a secret.
Number of Retransmits	The configured value of the maximum number of times a request packet is retransmitted.
Message Authenticator	A global parameter to indicate whether the Message Authenticator attribute is enabled or disabled.
Time Duration	The configured timeout value, in seconds, for request retransmissions.
RADIUS Accounting Mode	A global parameter to indicate whether the accounting mode for all the servers is enabled or not.
RADIUS Attribute 4 Mode	A global parameter to indicate whether the NAS-IP-Address attribute has been enabled to use in RADIUS requests.
RADIUS Attribute 4 Value	A global parameter that specifies the IP address to be used in NAS-IP-Address attribute used in RADIUS requests.

The following example shows CLI display output for the command.

```
(Extreme 220) #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
(Extreme 220) #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
(Extreme 220) #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
(Extreme 220) #show radius servers 192.168.37.58
Server Name..................................... Default_RADIUS_Server
Host Address.................................... 192.168.37.58
Secret Configured............................... No
Message Authenticator .......................... Enable
Number of Retransmits........................... 4
Time Duration................................... 10
RADIUS Accounting Mode.......................... Disable
RADIUS Attribute 4 Mode......................... Enable
RADIUS Attribute 4 Value ....................... 192.168.37.60
```

show radius accounting

This command displays a summary of configured *RADIUS* accounting servers.

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

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.

Column	Meaning
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.

The following example shows CLI display output for the command.

```
(Extreme 220) #show radius accounting name
Host Address            Server Name                       Port     Secret
                                                                   Configured
----------------------- --------------------------------- -------- -----------
192.168.37.200          Network1_RADIUS_Server            1813     Yes
192.168.37.201          Network2_RADIUS_Server            1813     No
192.168.37.202          Network3_RADIUS_Server            1813     Yes
192.168.37.203          Network4_RADIUS_Server            1813     No
 (Extreme 220) #show radius accounting name Default_RADIUS_Server
Server Name..............................  Default_RADIUS_Server
Host Address............................  192.168.37.200
RADIUS Accounting Mode..................  Disable
Port ...................................  1813
Secret Configured ......................  Yes
```

show radius accounting statistics

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

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

Column	Meaning
ipaddr	The IP address of the server.
dnsname	The DNS name of the server.

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

The following example shows CLI display output for the command.

```
(Extreme 220) #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
(Extreme 220) #show radius accounting statistics name Default_RADIUS_Server
RADIUS Accounting Server Name.................. Default_RADIUS_Server
Host Address................................... 192.168.37.200
Round Trip Time................................ 0.00
Requests....................................... 0
Retransmissions................................ 0
Responses...................................... 0
Malformed Responses............................ 0
Bad Authenticators............................. 0
Pending Requests............................... 0
Timeouts....................................... 0
```

```
Unknown Types.............................. 0
Packets Dropped............................ 0
```

show radius source-interface

Use this command in Privileged EXEC mode to display the configured *RADIUS* client source-interface (Source IP address) information.

Format	`show radius source-interface`
Mode	Privileged EXEC

The following example shows CLI display output for the command.

```
(Extreme 220) (Routing)# show radius source-interface
RADIUS Client Source Interface.............. (not configured)
```

show radius statistics

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

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

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

Column	Meaning
Pending Requests	The number of RADIUS Access-Request packets destined for this server that have not yet timed out or received a response.
Timeouts	The number of authentication timeouts to this server.
Unknown Types	The number of packets of unknown type that were received from this server on the authentication port.
Packets Dropped	The number of RADIUS packets received from this server on the authentication port and dropped for some other reason.

The following example shows CLI display output for the command.

```
(Extreme 220) #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
(Extreme 220) #show radius statistics name Default_RADIUS_Server
RADIUS Server Name..... Default_RADIUS_Server
Server Host Address..... 192.168.37.200
Access Requests..... 0.00
Access Retransmissions..... 0
Access Accepts..... 0
Access Rejects..... 0
Access Challenges..... 0
Malformed Access Responses..... 0
Bad Authenticators..... 0
Pending Requests..... 0
Timeouts..... 0
Unknown Types..... 0
Packets Dropped..... 0
```

TACACS+ Commands

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

tacacs-server host

Use this command in Global Configuration mode to configure a TACACS+ server. This command enters into the TACACS+ configuration mode. The ip-address|hostname parameter is the IP address or

hostname of the TACACS+ server. To specify multiple hosts, multiple tacacs-server host commands can be used.

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

no tacacs-server host

Use this command to delete the specified hostname or IP address. The `ip-address|hostname` parameter is the IP address of the TACACS+ server.

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

tacacs-server key

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

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

The ! (exclamation point) character cannot be used as the first character in a TACACS+ server password, unless the password is entered inside quotation marks from the CLI. We recommend using quotation marks whenever you create passwords and keys that contain the ! character – for example, `#tacacs-server key <"!234567">`.

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

no tacacs-server key

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

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

tacacs-server keystring

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

Format	`tacacs-server keystring`
Mode	Global Config

The following shows an example of this command.

```
(Extreme 220) (Config) #tacacs-server keystring
Enter tacacs key:********
Re-enter tacacs key:********
```

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 specific switch.

If a source-interface is not specified, the primary IP address of the originating (outbound) interface is used as the source address.

Format	`tacacs-server source-interface {`*`unit/slot/port`*`| loopback` *`loopback-id`* `| vlan` *`vlan-id`*`}`
Mode	Global Config

Parameter	Description
`unit/slot/port`	The unit identifier assigned to the switch, in unit/slot/port format.
`loopback-id`	The loopback interface. The range of the loopback ID is 0 to 7.
`vlan-id`	Configures the VLAN interface to use as the source IP address. The range of the VLAN ID is 1 to 4093.

The following shows an example of the command.

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

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.

Format	`no tacacs-server source-interface`
Mode	Global Config

tacacs-server timeout

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

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

no tacacs-server timeout

Use this command to restore the default timeout value for all TACACS servers.

Format	`no tacacs-server timeout`
Mode	Global Config

key

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

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

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

keystring

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

Format	`keystring`
Mode	TACACS Server Config

The following shows an example of the command.

```
(Extreme 220) (Config) #tacacs-server host 1.1.1.1
(Extreme 220)(Tacacs)#keystring
```

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

port

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

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

priority (TACACS Config)

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

Default	0
Format	`priority priority`
Mode	TACACS Config

timeout

Use this 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 (in seconds).

Format	`timeout timeout`
Mode	TACACS Config

show tacacs

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

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

Column	Meaning
Host address	The IP address or hostname of the configured TACACS+ server.
Port	The configured TACACS+ server port number.

Column	Meaning
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.

show tacacs source-interface

Use this 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.

Format	`show tacacs source-interface`
Mode	Privileged EXEC

The following example shows CLI display output for the command.

```
(Config)# show tacacs source-interface
TACACS Client Source Interface     : loopback 0
TACACS Client Source IPv4 Address  : 1.1.1.1 [UP]
```

Configuration Scripting Commands

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

Use the show running-config on page 159 command to capture the running configuration into a script. Use thecopy on page 189 command to transfer the configuration script to or from the switch.

Use the show on page 161command 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:

- Script files are not distributed across the stack, and only live in the unit that is the master unit at the time of the file download.
- The file extension must be ".scr".
- A maximum of ten scripts are allowed on the switch.
- The combined size of all script files on the switch cannot exceed 2048 KB.
- The maximum number of configuration file command lines is 2000.

You can type single-line annotations at the command prompt to use when you write test or configuration scripts to improve script readability. The exclamation point (!) character flags the beginning of a comment, and can begin a word anywhere on the command line, and all input following

this character is ignored. Any command line that begins with the "!" character is recognized as a comment line and ignored by the parser.

The following lines show an example of a script:

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

Note

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

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

script apply

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

Format	`script apply` *`scriptname`*
Mode	Privileged EXEC

script delete

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

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

script list

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

Format	`script list`
Mode	Privileged EXEC

Column	Meaning
Configuration Script	Name of the script.
Size	Privileged EXEC

script show

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

Format	`script show scriptname`
Mode	Privileged EXEC

Column	Meaning
Output Format	line *number*: *line contents*

script validate

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

Format	`script validate scriptname`
Mode	Privileged EXEC

Prelogin Banner, System Prompt, and Host Name Commands

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

copy (pre-login banner)

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

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

Default	None
Format	`copy tftp://{ipaddr/filepath/filename} nvram:clibanner` `copy nvram:clibanner tftp://{ipaddr/filepath/filename}`
Mode	Privileged EXEC

set prompt

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

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

hostname

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

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

show clibanner

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

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

The following example shows CLI display output for the command.

```
(Extreme 220) (Routing) #show clibanner
Banner Message configured :
==========================
--------------------------
         TEST
--------------------------
```

set clibanner

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

Format	`set clibanner line`
Mode	Global Config

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

no set clibanner

Use this command to unconfigure the prelogin CLI banner.

Format	`no set clibanner`
Mode	Global Config

4 Utility Commands

This chapter describes the utility commands available in the 200 Series CLI.

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

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

AutoInstall Commands

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

AutoInstall includes the following support:

- Downloading an image from TFTP server using *DHCP (Dynamic Host Configuration Protocol)* option 125. The image update can result in a downgrade or upgrade of the firmware on the switch.

- Automatically downloading a configuration file from a TFTP server when the switch is booted with no saved configuration file.
- Automatically downloading an image from a TFTP server in the following situations:
  - When the switch is booted with no saved configuration found.
  - When the switch is booted with a saved configuration that has AutoInstall enabled.

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

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

Note

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

boot autoinstall

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

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

boot host retrycount

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

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

no boot host retrycount

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

Format	`no boot host retrycount`
Mode	Privileged EXEC

boot host dhcp

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

Default	enabled
Format	`boot host dhcp`
Mode	Privileged EXEC

no boot host dhcp

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

Format	`no boot host dhcp`
Mode	Privileged EXEC

boot host autosave

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

Default	Disabled
Format	`boot host autosave`
Mode	Privileged EXEC

no boot host autosave

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

Format	`no boot host autosave`
Mode	Privileged EXEC

boot host autoreboot

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

Default	Enabled
Format	`boot host autoreboot`
Mode	Privileged EXEC

no boot host autoreboot

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

Format	`no boot host autoreboot`
Mode	Privileged EXEC

erase startup-config

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

Format	`erase startup-config`
Mode	Privileged EXEC

erase factory-defaults

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

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

show autoinstall

This command displays the current status of the AutoInstall process.

Format	`show autoinstall`
Mode	Privileged EXEC

The following example shows CLI display output for the command.

```
(Extreme 220) #show autoinstall
AutoInstall Mode.............................. Stopped
AutoInstall Persistent Mode................... Disabled
AutoSave Mode................................. Disabled
AutoReboot Mode............................... Enabled
AutoInstall Retry Count....................... 3
```

CLI Output Filtering Commands

In each of the following command descriptions, *xxx* represents any valid parameter for the `show` command – for example, *`interface`* or *`running-config`*.

show xxx|include “string”

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

The following shows an example of this command.

```
(Extreme 220) (Routing) #show running-config | include “spanning-tree”
spanning-tree configuration name "00-02-BC-42-F9-33"
spanning-tree bpduguard
spanning-tree bpdufilter default
```

show xxx|include “string” exclude “string2”

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

The following example shows of the CLI command.

```
(Extreme 220) (Routing) #show running-config | include “spanning-tree” exclude
“configuration”
spanning-tree bpduguard
spanning-tree bpdufilter default
```

show xxx|exclude “string”

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

The following shows an example of this command.

```
(Extreme 220) (Routing) #show interface 0/1
Packets Received Without Error..................... 0
Packets Received With Error........................ 0
Broadcast Packets Received......................... 0
Receive Packets Discarded.......................... 0
Packets Transmitted Without Errors................. 0
Transmit Packets Discarded......................... 0
Transmit Packet Errors............................. 0
Collision Frames................................... 0
Time Since Counters Last Cleared................... 281 day 4 hr 9 min 0 sec
(Extreme 220) (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
```

show xxx|begin “string”

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

The following shows an example of this command.

```
(Extreme 220) (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
(Extreme 220) (Routing) #
```

show xxx|section "string"

The command 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 (that is, "exit").

The following shows an example of this command.

```
(Extreme 220) (Routing) #show running-config | section "interface 0/1"
interface 0/1
no spanning-tree port mode
exit
```

show xxx|section "string" "string2"

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

show xxx|section "string" include "string2"

The command 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 (that is, "exit") and that include the "string2" match. This type of filter command could also include "exclude" or user-defined end-of-section identifier parameters as well.

Dual Image Commands

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

The 200 Series 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 downtime when you upgrade or downgrade the software.

delete

This command deletes the backup image file from the permanent storage or the core dump file from the local file system. The optional unit parameter is valid only on stacks. An error will be returned, if this parameter is provided, on Standalone systems. In a stack, the unit parameter identifies the node on which this command must be executed. When this parameter is not supplied, the command is executed on all nodes in a stack.

Format	`delete [unit] backup` `delete core-dump-file file-name | all`
Mode	Privileged EXEC

boot system

This command activates the specified image. It will be the active-image for subsequent reboots and will be loaded by the boot loader. The current active-image is marked as the backup-image for subsequent reboots. If the specified image doesn't exist on the system, this command returns an error message. The optional unit parameter is valid only in Stacking, where the unit parameter identifies the node on which this command must be executed. When this parameter is not supplied, the command is executed on all nodes in a stack.

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

show bootvar

This command displays the version information and the activation status for the current active and backup images on the supplied unit (node) of the stack. If you do not specify a unit number, the command displays image details for all nodes on the stack. The command also displays any text description associated with an image. This command, when used on a standalone system, displays the switch activation status. For a standalone system, the unit parameter is not valid.

Format	`show bootvar [unit]`
Mode	Privileged EXEC

filedescr

This command associates a given text description with an image. Any existing description will be replaced. The command is executed on all nodes in a stack.

Format	`filedescr {active | backup} text-description`
Mode	Privileged EXEC

update bootcode

This command updates the bootcode (boot loader) on the switch. The bootcode is read from the active-image for subsequent reboots.The optional unit parameter is valid only on stacks. An error will be returned, if this parameter is provided, on standalone systems. For stacking, the unit parameter identifies the node on which this command must be executed. When this parameter is not supplied, the command is executed on all nodes in a stack.

Format	`update bootcode [unit]`
Mode	Privileged EXEC

System Information and Statistics Commands

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

load-interval

This command changes the length of time for which data is used to compute load statistics. The value is given in seconds, and must be a multiple of 30. The allowable range for interval is from 30 to 600 seconds. The smaller the value of the load interval is, the more accurate is the instantaneous rate given by load statistics. Smaller values may affect system performance.

Default	300
Format	`load-interval interval`
Mode	Interface Config

```
(Extreme 220) (Interface 0/1)#load-interval 30
```

no load-interval

This command resets the load interval on the interface to the default value.

Format	`load-interval interval`
Mode	Interface Config

show arp switch

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

Format	`show arp switch`
Mode	Privileged EXEC

Column	Meaning
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.

show eventlog

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

Format	`show eventlog [unit]`
Mode	Privileged EXEC

Column	Meaning
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.
Unit	The unit for the event.

Note
Event log information is retained across a switch reboot.

show hardware

This command displays inventory information for the switch.

Note
The `show version` command and the `show hardware` command display the same information. In future releases of the software, the `show hardware` command will not be available. For a description of the command output, see the command show version on page 143.

Format	`show hardware`
Mode	Privileged EXEC

show version

This command displays inventory information for the switch.

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

Format	`show version`
Mode	Privileged EXEC

Column	Meaning
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.
Burned in MAC Address	Universally assigned network address.
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.
Network Processing Device	The type of the processor microcode.
Additional Packages	The additional packages incorporated into this system.

show platform vpd

This command displays vital product data for the switch.

Format	`show platform vpd`
Mode	User Privileged

The following information is displayed:

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

The following example shows CLI display output for the command.

```
(Extreme 220) (Routing) #show platform vpd
Operational Code Image File Name.............. FastPath-Ent-esw-xgs4-gto-BL20R-
```

```
CS-6AIQHSr3v7m14b35
Software Version.............................. 3.7.14.35
Timestamp..................................... Thu Mar  7 14:36:14 IST 2013
```

show interface

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

Format	`show interface {`*`unit/slot/port`* `| switchport | lag` *`lag-id`*`}`
Mode	Privileged EXEC

The display parameters, when the argument is unit/slot/port or lag lag-id, are as follows:

Column	Meaning
Packets Received Without Error	The total number of packets (including broadcast packets and multicast packets) received by the processor.
Packets Received With Error	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Broadcast Packets Received	The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.
Receive Packets Discarded	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffered space.
Packets Transmitted Without Error	The total number of packets transmitted out of the interface.
Transmit Packets Discarded	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. A possible reason for discarding a packet could be to free up buffer space.
Transmit Packets Errors	The number of outbound packets that could not be transmitted because of errors.
Collisions Frames	The best estimate of the total number of collisions on this Ethernet segment.
Load Interval	The length of time for which data is used to compute load statistics. The value is given in seconds, and must be a multiple of 30. The allowable range is from 30 to 600 seconds
Bits Per Second Received	Approximate number of bits per second received. This value is an exponentially weighted average and is affected by the configured load-interval.
Bits Per Second Transmitted.	Approximate number of bits per second transmitted. This value is an exponentially weighted average and is affected by the configured load-interval.
Packets Per Second Received	Approximate number of packets per second received. This value is an exponentially weighted average and is affected by the configured load-interval.
Packets Per Second Transmitted	Approximate number of packets per second transmitted. This value is an exponentially weighted average and is affected by the configured load-interval.
Percent Utilization Received	Value of link utilization in percentage representation for the RX line.
Percent Utilization Transmitted	Value of link utilization in percentage representation for the TX line.

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

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

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

show interfaces status

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

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

Format	`show interfaces status [{`*`unit/slot/port`* `|` **`vlan`** *`id`*`}]`
Mode	Privileged EXEC

Column	Meaning
Port	The interface associated with the rest of the data in the row.
Name	The descriptive user-configured name for the interface.
Link State	Whether the link is up or down.
Physical Mode	The speed and duplex settings on the interface.
Physical Status	The port speed and duplex mode for physical interfaces. The physical status for LAGs is not reported. When a port is down, the physical status is unknown.
Media Type	The media type of the interface.

Column	Meaning
Flow Control Status	The 802.3x flow control status.
Flow Control	The configured 802.3x flow control mode.

show interfaces traffic

Use this command to display interface traffic information.

Format	`show interfaces traffic [unit/slot/port]`
Mode	Privileged EXEC

Column	Meaning
Interface Name	The interface associated with the rest of the data in the row.
Congestion Drops	The number of packets that have been dropped on the interface due to congestion.
TX Queue	The number of cells in the transmit queue.
RX Queue	The number of cells in the receive queue.
Color Drops: Yellow	The number of yellow (conformed) packets that were dropped.
Color Drops: Red	The number of red (exceeded) packets that were dropped.
WRED TX Queue	The number of packets in the WRED transmit queue.

show interface counters

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

Format	`show interface counters`
Mode	Privileged EXEC

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

The following example shows CLI display output for the command.

```
(Extreme 220) (Routing) #show interface counters
Port              InOctets      InUcastPkts      InMcastPkts      InBcastPkts
```

```
--------- ---------------- ---------------- ---------------- ----------------
0/1                     0                0                0                0
Port              InOctets      InUcastPkts      InMcastPkts      InBcastPkts
--------- ---------------- ---------------- ---------------- ----------------
0/1                  0             0                0                0
0/2                  0             0                0                0
0/3              15098             0                31               39
0/4                  0             0                0                0
0/5                  0             0                0                0
...
...
ch1                  0             0                0                0
ch2                  0             0                0                0
...
ch64                 0             0                0                0
CPU                359533          0                3044             217
Port             OutOctets     OutUcastPkts     OutMcastPkts     OutBcastPkts
--------- ---------------- ---------------- ---------------- ----------------
0/1                  0             0                0                0
0/2                  0             0                0                0
0/3                131369          0                11               89
0/4                  0             0                0                0
0/5                  0             0                0                0
...
...
ch1                  0             0                0                0
ch2                  0             0                0                0
...
ch64                 0             0                0                0
CPU              4025293           0                32910            120
```

show interface ethernet

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

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

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

Column	Meaning
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).

Column	Meaning
	• Packets Received 256–511 Octets - The total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets). • Packets Received 512–1023 Octets - The total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets). • Packets Received 1024–1518 Octets - The total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets). • Packets Received > 1518 Octets - The total number of packets received that were longer than 1522 octets (excluding framing bits, but including FCS octets) and were otherwise well formed. • 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 Received(con't)	• Packets RX and TX 512–1023 Octets - The total number of packets (including bad packets) received and transmitted that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets). • Packets RX and TX 1024–1518 Octets - The total number of packets (including bad packets) received and transmitted that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets). • Packets RX and TX 1519–2047 Octets - The total number of packets received and transmitted that were between 1519 and 2047 octets in length inclusive (excluding framing bits, but including FCS octets) and were otherwise well formed. • Packets RX and TX 1523–2047 Octets - The total number of packets received and transmitted that were between 1523 and 2047 octets in length inclusive (excluding framing bits, but including FCS octets) and were otherwise well formed. • Packets RX and TX 2048–4095 Octets - The total number of packets received that were between 2048 and 4095 octets in length inclusive (excluding framing bits, but including FCS octets) and were otherwise well formed. • Packets RX and TX 4096–9216 Octets - The total number of packets received that were between 4096 and 9216 octets in length inclusive (excluding framing bits, but including FCS octets) and were otherwise well formed.
Packets Received Successfully	• Total Packets Received Without Error - The total number of packets received that were without errors. • Unicast Packets Received - The number of subnetwork-unicast packets delivered to a higher-layer protocol. • Multicast Packets Received - The total number of good packets received that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address. • Broadcast Packets Received - The total number of good packets received that were directed to the broadcast address. Note that this does not include multicast packets.

Column	Meaning
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 total number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol. • Jabbers Received - The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). Note that this definition of jabber is different than the definition in IEEE-802.3 section 8.2.1.5 (10BASE5) and section 10.3.1.4 (10BASE2). These documents define jabber as the condition where any packet exceeds 20 ms. The allowed range to detect jabber is between 20 ms and 150 ms. • Fragments/Undersize Received - The total number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets). • Alignment Errors - The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with a non-integral number of octets. • FCS Errors - The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with an integral number of octets. • Overruns - The total number of frames discarded as this port was overloaded with incoming packets, and could not keep up with the inflow.
Received Packets Not Forwarded	• Total Received Packets Not Forwarded - A count of valid frames received which were discarded (in other words, filtered) by the forwarding process • 802.3x Pause Frames Received - A count of MAC Control frames received on this interface with an opcode indicating the PAUSE operation. This counter does not increment when the interface is operating in half-duplex mode. • Unacceptable Frame Type - The number of frames discarded from this port due to being an unacceptable frame type.
Packets Transmitted Octets	• Total Packets Transmitted (Octets) - The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets). This object can be used as a reasonable estimate of Ethernet utilization. If greater precision is desired, the etherStatsPkts and etherStatsOctets objects should be sampled before and after a common interval. ----- • Packets Transmitted 64 Octets - The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets). • Packets Transmitted 65-127 Octets - The total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets). • Packets Transmitted 128-255 Octets - The total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets). • Packets Transmitted 256-511 Octets - The total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets). • Packets Transmitted 512-1023 Octets - The total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).

Column	Meaning
	• Packets Transmitted 1024-1518 Octets - The total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets). • Packets Transmitted > 1518 Octets - The total number of packets transmitted that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed. • Max Frame Size - The maximum size of the Info (non-MAC) field that this port will receive or transmit. • Maximum Transmit Unit - The maximum Ethernet payload size.
Packets Transmitted Successfully	• Total Packets Transmitted Successfully- The number of frames that have been transmitted by this port to its segment. • Unicast Packets Transmitted - The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent. • Multicast Packets Transmitted - The total number of packets that higher-level protocols requested be transmitted to a Multicast address, including those that were discarded or not sent. • Broadcast Packets Transmitted - The total number of packets that higher-level protocols requested be transmitted to the Broadcast address, including those that were discarded or not sent.
Transmit Packets Discarded	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. A possible reason for discarding a packet could be to free up buffer space.
Transmit Errors	• Total Transmit Errors - The sum of Single, Multiple, and Excessive Collisions. • FCS Errors - The total number of packets transmitted that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with an integral number of octets. • Underrun Errors - The total number of frames discarded because the transmit FIFO buffer became empty during frame transmission.
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. • GVRP PDUs Received - The count of GVRP PDUs received in the GARP layer. • GVRP PDUs Transmitted - The count of GVRP PDUs transmitted from the GARP layer. • GVRP Failed Registrations - The number of times attempted GVRP registrations could not be completed. • GMRP PDUs Received - The count of GMRP PDUs received in the GARP layer. • GMRP PDUs Transmitted - The count of GMRP PDUs transmitted from the GARP layer.

Column	Meaning
	• GMRP Failed Registrations - The number of times attempted GMRP registrations could not be completed. • STP BPDUs Transmitted - Spanning Tree Protocol Bridge Protocol Data Units sent. • STP BPDUs Received - Spanning Tree Protocol Bridge Protocol Data Units received. • RST BPDUs Transmitted - Rapid Spanning Tree Protocol Bridge Protocol Data Units sent. • RSTP BPDUs Received - Rapid Spanning Tree Protocol Bridge Protocol Data Units received. • MSTP BPDUs Transmitted - Multiple Spanning Tree Protocol Bridge Protocol Data Units sent. • MSTP BPDUs Received - Multiple Spanning Tree Protocol Bridge Protocol Data Units received. • SSTP BPDUs Transmitted - Shared Spanning Tree Protocol Bridge Protocol Data Units sent. • SSTP BPDUs Received - Shared 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 Start Frames Received - The number of valid EAPOL start frames that have been received by this authenticator.
Traffic Load Statistics	• Load Interval - The length of time for which data is used to compute load statistics. The value is given in seconds, and must be a multiple of 30. The allowable range is from 30 to 600 seconds • Bits Per Second Received - Approximate number of bits per second received. This value is an exponentially weighted average and is affected by the configured load-interval. • Bits Per Second Transmitted. - Approximate number of bits per second transmitted. This value is an exponentially weighted average and is affected by the configured load-interval. • Packets Per Second Received- Approximate number of packets per second received. This value is an exponentially weighted average and is affected by the configured load-interval. • Packets Per Second Transmitted - Approximate number of packets per second transmitted. This value is an exponentially weighted average and is affected by the configured load-interval. • Percent Utilization Received - Value of link utilization in percentage representation for the RX line. • Percent Utilization Transmitted - Value of link utilization in percentage representation for the TX line.
Time Since Counters Last Cleared	The elapsed time, in days, hours, minutes, and seconds since the statistics for this port were last cleared.

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

Column	Meaning
Packets Received Without Error	The total number of packets (including broadcast packets and multicast packets) received by the processor.
Broadcast Packets Received	The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.
Packets Received With Error	The total number of packets with errors (including broadcast packets and multicast packets) received by the processor.
Packets Transmitted without Errors	The total number of packets transmitted out of the interface.

Column	Meaning
Broadcast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to the Broadcast address, including those that were discarded or not sent.
Transmit Packet Errors	The number of outbound packets that could not be transmitted because of errors.
Time Since Counters Last Cleared	The elapsed time, in days, hours, minutes, and seconds, since the statistics for this switch were last cleared.

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

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

show interface ethernet switchport

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

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

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

The command displays the following information.

Column	Meaning
Private-vlan host-association	The VLAN association for the private-VLAN host ports.
Private-vlan mapping	The VLAN mapping for the private-VLAN promiscuous ports.

show interface lag

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

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

Column	Meaning
Packets Received Without Error	The total number of packets (including broadcast packets and multicast packets) received on the LAG interface
Packets Received With Error	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.

Column	Meaning
Broadcast Packets Received	The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.
Receive Packets Discarded	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
Packets Transmitted Without Error	The total number of packets transmitted out of the LAG.
Transmit Packets Discarded	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. A possible reason for discarding a packet could be to free up buffer space.
Transmit Packets Errors	The number of outbound packets that could not be transmitted because of errors.
Collisions Frames	The best estimate of the total number of collisions on this Ethernet segment.
Time Since Counters Last Cleared	The elapsed time, in days, hours, minutes, and seconds since the statistics for this LAG were last cleared.

show fiber-ports optical-transceiver

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

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

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

The following shows an example of the command output:

```
(Extreme 220) #show fiber-ports optical-transceiver all
                                        Output    Input
Port      Temp  Voltage  Current       Power     Power    TX     LOS
           [C]   [Volt]     [mA]       [dBm]     [dBm]   Fault
--------  ----  -------  -------    -------   -------   -----  ---
0/49      39.3    3.256      5.0     -2.234    -2.465   No     No
0/50      33.9    3.260      5.3     -2.374   -40.000   No     Yes
0/51      32.2    3.256      5.6     -2.300    -2.897   No     No
```

show fiber-ports optical-transceiver-info

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

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

Column	Meaning
Vendor Name	The vendor name is a 16 character field that contains ASCII characters, left-aligned and padded on the right with ASCII spaces (20h). The vendor name should be the full name of the corporation, a commonly accepted abbreviation of the name of the corporation, the SCSI company code for the corporation, or the stock exchange code for the corporation.
Length (50um, OM2)	This value specifies link length that is supported by the transceiver while operating in compliance with applicable standards using 50 micron multimode OM2 [500MHz*km at 850nm] fiber. A value of zero means that the transceiver does not support 50 micron multimode fiber or that the length information must be determined from the transceiver technology.
Length (62.5um, OM1)	This value specifies link length that is supported by the transceiver while operating in compliance with applicable standards using 62.5 micron multimode OM1 [200 MHz*km at 850nm, 500 MHz*km at 1310nm] fiber. A value of zero means that the transceiver does not support 62.5 micron multimode fiber or that the length information must determined from the transceiver technology
Vendor SN	The vendor serial number (vendor SN) is a 16 character field that contains ASCII characters, left-aligned and padded on the right with ASCII spaces (20h), defining the vendor's serial number for the transceiver. A value of all zero in the 16-byte field indicates that the vendor SN is unspecified.
Vendor PN	The vendor part number (vendor PN) is a 16-byte field that contains ASCII characters, left aligned and added on the right with ASCII spaces (20h), defining the vendor part number or product name. A value of all zero in the 16-byte field indicates that the vendor PN is unspecified.
BR, nominal	The nominal bit (signaling) rate (BR, nominal) is specified in units of 100 MBd, rounded off to the nearest 100 MBd. The bit rate includes those bits necessary to encode and delimit the signal as well as those bits carrying data information. A value of 0 indicates that the bit rate is not specified and must be determined from the transceiver technology. The actual information transfer rate will depend on the encoding of the data, as defined by the encoding value.
Vendor Rev	The vendor revision number (vendor rev) contains ASCII characters, left aligned and padded on the right with ASCII spaces (20h), defining the vendor's product revision number. A value of all zero in this field indicates that the vendor revision is unspecified.

The following shows an example of the command output:

```
(Extreme 220) #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  Compliance
-------- --------------- --- ---- ---------------- ---------------- ------ ---- -----------
1/0/25   Siemon          0   0    1420X-40138      900074-10-02     10300 C    DAC
1/0/26   Siemon          0   0    1420X-40142      900074-10-02     10300 C    DAC
2/0/49   Siemon          0   0    1420X-40138      900074-10-02     10300 C    DAC
2/0/50   Siemon          0   0    1420X-40142      900074-10-02     10300 C    DAC
```

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 parameter to view MAC addresses on a specific interface.

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. Use the vlan vlan_id parameter to display information about MAC addresses on a specified VLAN.

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

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

Column	Meaning
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 ifIndex of the interface table entry associated with this port.
Status	The status of this entry. The meanings of the values are: • *Static*—The value of the corresponding instance was added by the system or a user when a static MAC filter was defined. It cannot be relearned. • *Learned*—The value of the corresponding instance was learned by observing the source MAC addresses of incoming traffic, and is currently in use. • *Management*—The value of the corresponding instance (system MAC address) is also the value of an existing instance of dot1dStaticAddress. It is identified with interface 0/1. and is currently used when enabling VLANs for routing. • *Self*—The value of the corresponding instance is the address of one of the switch's physical interfaces (the system's own MAC address). • *GMRP Learned*—The value of the corresponding was learned via GMRP and applies to Multicast. • *Other*—The value of the corresponding instance does not fall into one of the other categories.

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

The following information displays if you enter the count parameter:

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

process cpu threshold

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

Format	`process cpu threshold type total rising` *`rising-threshold`* `interval` *`rising-interval`* `[falling` *`falling-threshold`* `interval` *`falling-interval`*`]`
Mode	Global Config

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

show process app-list

This command displays the user and system applications.

Note
This command is available in Linux 2.6 only.

Format	show process app-list
Mode	Privileged EXEC

Column	Meaning
ID	The application identifier.
Name	The name that identifies the process.
PID	The number the software uses to identify the process.
Admin Status	The administrative status of the process.
Auto Restart	Whether the process will automatically restart if it stops.
Running Status	Whether the process is currently running or stopped.

The following example shows CLI display output for the command.

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

show process app-resource-list

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

Note
This command is available in Linux 2.6 only.

Format	show process app-resource-list
Mode	Privileged EXEC

Column	Meaning
ID	The application identifier.
Name	The name that identifies the process.
PID	The number the software uses to identify the process.
Memory Limit	The maximum amount of memory the process can consume.
CPU Share	The maximum percentage of CPU utilization the process can consume.
Memory Usage	The amount of memory the process is currently using.
Max Mem Usage	The maximum amount of memory the process has used at any given time since it started.

The following example shows CLI display output for the command.

```
(Extreme 220) (Routing) #show process app-resource-list
                            Memory      CPU       Memory      Max Mem
ID   Name              PID  Limit       Share     Usage       Usage
---- ---------------- ---- ----------- --------- ----------- -----------
   1 switchdrvr        251   Unlimited Unlimited      380 MB      381 MB
   2 syncdb            252   Unlimited Unlimited        0 MB        0 MB
   3 syncdb-test         0   Unlimited Unlimited        0 MB        0 MB
   4 proctest            0       10 MB       20%        0 MB        0 MB
   5 utelnetd            0   Unlimited Unlimited        0 MB        0 MB
   6 lxshTelnetd         0   Unlimited Unlimited        0 MB        0 MB
   7 user.start          0   Unlimited Unlimited        0 MB        0 MB
```

show process cpu

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

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

Note
This command is available in Linux 2.6 only.

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

Column	Meaning
Free	System wide free memory
Alloc	System wide allocated memory (excluding cache, file system used space)
Pid	Process or Thread Id
Name	Process or Thread Name
5Secs	CPU utilization sampling in 5Secs interval
60Secs	CPU utilization sampling in 60Secs interval
300Secs	CPU utilization sampling in 300Secs interval
Total CPU Utilization	Total CPU utilization % within the specified window of 5Secs, 60Secs and 300Secs.

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

```
(Extreme 220) (Routing) #show process cpu
Memory Utilization Report
status      bytes
------ ----------
free    106450944
alloc   423227392
 CPU Utilization:
  PID      Name                    5 Secs     60 Secs    300 Secs
--------------------------------------------------------------------
  765    _interrupt_thread          0.00%       0.01%       0.02%
  767    bcmL2X.0                   0.58%       0.35%       0.28%
  768    bcmCNTR.0                  0.77%       0.73%       0.72%
  773    bcmRX                      0.00%       0.04%       0.05%
  786    cpuUtilMonitorTask         0.19%       0.23%       0.23%
```

```
  834    dot1s_task                0.00%       0.01%       0.01%
  810    hapiRxTask                0.00%       0.01%       0.01%
  805    dtlTask                   0.00%       0.02%       0.02%
  863    spmTask                   0.00%       0.01%       0.00%
  894    ip6MapLocalDataTask       0.00%       0.01%       0.01%
  908    RMONTask                  0.00%       0.11%       0.12%
-------------------------------------------------------------------
Total CPU Utilization              1.55%       1.58%       1.50%
```

show process proc-list

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

Note
This command is available in Linux 2.6 only.

Format	`show process proc-list`
Mode	Privileged EXEC

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

The following example shows CLI display output for the command.

```
(Extreme 220) (Routing) #show process proc-list
      Process          Application                VM Size  VM Peak
PID   Name             ID-Name               Chld  (KB)      (KB)     FD Count
---- ---------------- --------------------- ---- -------- -------- --------
15260 procmgr           0-procmgr             No       1984     1984         8
15309 dataplane         1-dataplane           No     293556   293560        11
15310 switchdrvr        2-switchdrvr          No     177220   177408        57
15314 syncdb            3-syncdb              No       2060     2080         8
18718 lighttpd          4-lighttpd            No       5508     5644        11
18720 lua_magnet        4-lighttpd            Yes     12112    12112         7
18721 lua_magnet        4-lighttpd            Yes     25704    25708         7
```

show running-config

Use this command to display or capture the current setting of different protocol packages supported on the switch. This command displays or captures commands with settings and configurations that differ

from the default value. To display or capture the commands with settings and configurations that are equal to the default value, include the all option.

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

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

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

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

Use the following keys to navigate the command output.

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

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

This command captures the current settings of OSPFv2 and *OSPFv3 (Open Shortest Path First version 3)* trapflag status:

- If all the flags are enabled, then the command displays trapflags all.
- If all the flags in a particular group are enabled, then the command displays trapflags group name all.
- If some, but not all, of the flags in that group are enabled, the command displays trapflags groupname flag-name.

Format	`show running-config [all | scriptname]`
Mode	Privileged EXEC

show running-config interface

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

Format	`show running-config interface {`*`interface`*` | lag {`*`lag-intf-num`*`} | loopback {`*`loopback-id`*`} | vlan {`*`vlan-id`*`}}`
Mode	Privileged EXEC

Parameter	Description
interface	Running configuration for the specified interface.
lag-intf-num	Display the running config for a specified LAG interface.
loopback-id	Display the running config for a specified loopback interface.
vlan-id	Display the running config for a specified vlan routing interface.

The following example shows CLI display output for the command.

```
(Extreme 220) (Routing) #show running-config interface 0/1
!Current Configuration:
!
interface  0/1
addport 3/1
exit
(Extreme 220) (Routing) #
```

show

This command displays the content of text-based configuration files from the CLI. The text-based configuration files (startup-config, backup-config and factory-defaults) are saved compressed in flash. With this command, the files are decompressed while displaying their content.

Format	`show {startup-config | backup-config | factory-defaults}`
Mode	Privileged EXEC

Parameter	Description
startup-config	Display the content of the startup-config file.
backup-config	Display the content of the backup-config file.
factory-defaults	Display the content of the factory-defaults file.

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

```
(Extreme 220) (Routing) #show startup-config
!Current Configuration:
!
!System Description "Extreme 220-Series 24GE, 2 10GbE SFP+ ports, 1 Fixed AC PSU
, 1 RPS port, L3 Switching, 1.1.50.6, Linux 3.6.5, U-Boot 2012.10-gac78d49 (Jan
09 2017 - 11:09:03)"
!System Software Version "1.1.50.6"
!System Up Time          "0 days 1 hrs 35 mins 29 secs"
```

```
!Additional Packages     FASTPATH QOS,FASTPATH IPv6 Management,FASTPATH Stacking
,FASTPATH Routing
!Current SNTP Synchronized Time: SNTP Client Mode Is Disabled
!
serviceport protocol none
serviceport ip 10.50.3.138 255.255.254.0 10.50.2.1
vlan database
exit
ip ssh server enable
configure
stack
member 1 3
exit
ip host "devices.extremenetworks.com" 10.49.72.138
slot 1/0 3
set slot power 1/0
no set slot disable 1/0
username "nms" password 406a25922efd849329406439d6ce2eadd2f59c4e2f25a6cc92f6bbe3
31d53ed8b7848defc4c002f7b639a0633e21951ef68a537451d7afea33114ac350acbf9b level 1
5 encrypted
line console
exit
line telnet
exit
line ssh
exit
!
snmp-server community "ExtremeNMS" ro ipaddress 134.141.5.175
dot1as
router rip
exit
exit
```

dir

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

Format	`dir`
Mode	Privileged EXEC

```
(Extreme 220) (Routing) #dir
    0  drwx                2048 May 09 2002 16:47:30 .
    0  drwx                2048 May 09 2002 16:45:28 ..
    0  -rwx                592 May 09 2002 14:50:24 slog2.txt
    0  -rwx                72 May 09 2002 16:45:28 boot.dim
    0  -rwx                 0 May 09 2002 14:46:36 olog2.txt
    0  -rwx                 13376020 May 09 2002 14:49:10 image1
    0  -rwx                 0 Apr 06 2001 19:58:28 fsyssize
    0  -rwx                1776 May 09 2002 16:44:38 slog1.txt
    0  -rwx                 356 Jun 17 2001 10:43:18 crashdump.ctl
    0  -rwx                1024 May 09 2002 16:45:44 sslt.rnd
    0  -rwx                14328276 May 09 2002 16:01:06 image2
    0  -rwx                 148 May 09 2002 16:46:06 hpc_broad.cfg
    0  -rwx                   0 May 09 2002 14:51:28 olog1.txt
    0  -rwx                 517 Jul 23 2001 17:24:00 ssh_host_key
    0  -rwx                69040 Jun 17 2001 10:43:04 log_error_crashdump
    0  -rwx                 891 Apr 08 2000 11:14:28 sslt_key1.pem
    0  -rwx                 887 Jul 23 2001 17:24:00 ssh_host_rsa_key
    0  -rwx                 668 Jul 23 2001 17:24:34 ssh_host_dsa_key
    0  -rwx                 156 Apr 26 2001 13:57:46 dh512.pem
```

```
    0  -rwx                  245 Apr 26 2001 13:57:46 dh1024.pem
    0  -rwx                    0 May 09 2002 16:45:30 slog0.txt
```

show sysinfo

This command displays switch information.

Format	show sysinfo
Mode	Privileged EXEC

Column	Meaning
Switch Description	Text used to identify this switch.
System Name	Name used to identify the switch.The factory default is blank. To configure the system name, see snmp-server on page 92.
System Location	Text used to identify the location of the switch. The factory default is blank. To configure the system location, see snmp-server on page 92.
System Contact	Text used to identify a contact person for this switch. The factory default is blank. To configure the system location, see snmp-server on page 92.
System ObjectID	The base object ID for the switch's enterprise MIB.
System Up Time	The time in days, hours and minutes since the last switch reboot.
Current SNTP Synchronized Time	The system time acquired from a network *SNTP (Simple Network Time Protocol)* server.
MIBs Supported	A list of MIBs supported by this agent.

show tech-support

Use the show tech-support command to display system and configuration information when you contact technical support. The output of the show tech-support command combines the output of the following commands and includes log history files from previous runs:

- `show version`
- `show sysinfo`
- `show port all`
- `show isdp neighbors`
- `show logging`
- `show event log`
- `show logging buffered`
- `show msg-queue`
- `show trap log`
- `show running-config`

Including the optional ospf parameter also displays OSPF information.

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

length value

Use this command to set the pagination length (number of lines) for the sessions specified by configuring on different Line Config modes (telnet/ssh/console). This setting is persistent.

Valid values are 0 (no lines) and 5 through 48.

Default	24
Format	`length` *`value`*
Mode	Line Config

The `length` command on Line Console mode also applies for Serial Console sessions.

no length value

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

Format	`no length` *`value`*
Mode	Line Config

terminal length

Use this command to set the pagination length to value number of lines for the current session. This command configuration takes an immediate effect on the current session and is nonpersistent.

Default	24 lines per page
Format	`terminal length` *`value`*
Mode	Privileged EXEC

no terminal length

Use this command to set the value to the length value configured on Line Config mode depending on the type of session.

Format	`no terminal length` *`value`*
Mode	Privileged EXEC

show terminal length

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

Format	`show terminal length`
Mode	Privileged EXEC

The following example shows CLI display output for the command.

```
(Extreme 220) (Routing) #show terminal length
Terminal Length:
----------------------
For Current Session..... 24
For Serial Console..... 24
For Telnet Sessions..... 24
For SSH Sessions..... 24
```

memory free low-watermark processor

Use this command to get notifications when the CPU free memory falls below the configured threshold. A notification is generated when the free memory falls below the threshold. Another notification is generated once the available free memory rises to 10 percent above the specified threshold. To prevent generation of excessive notifications when the CPU free memory fluctuates around the configured threshold, only one Rising or Falling memory notification is generated over a period of 60 seconds. The threshold is specified in kilobytes. The CPU free memory threshold configuration is saved across a switch reboot.

Format	`memory free low-watermark processor 1-1034956`
Mode	Global Config

Parameter	Description
`low-watermark`	When CPU free memory falls below this threshold, a notification message is triggered. The range is 1 to the maximum available memory on the switch. The default is 0 (disabled).

clear mac-addr-table

Use this command to dynamically clear learned entries from the forwarding database. Using the following options, the user can specify the set of dynamically-learned forwarding database entries to clear.

Default	No default value.
Format	`clear mac-addr-table {all | vlan` *`vlanId`* `| interface` *`unit/slot/port`* `|` *`macAddr`* `[`*`macMask`*`]}`
Mode	Privileged EXEC

Parameter	Description
`all`	Clears dynamically learned forwarding database entries in the forwarding database table.
vlan *`vlanId`*	Clears dynamically learned forwarding database entries for this vlanId.

Parameter	Description
unit/slot/port	Clears forwarding database entries learned on for the specified interface.
macAddr macMask	Clears dynamically learned forwarding database entries that match the range specified by MAC address and MAC mask. When MAC mask is not entered, only specified MAC is removed from the forwarding database table.

Box Services Commands

This section describes the Box Services commands. Box services are services that provide support for features such as temperature, power supply status, fan control, and others. Each of these services is platform dependent. (For example, some platforms may have temperature sensors, but no fan controller. Or, others may have both while others have neither.)

Note
The bootloader version can only be supported on PowerPC platforms that use the u-boot loader.

show version bootloader

Use this command to display Uboot version information.

Format	`show version bootloader`
Mode	Privileged EXEC

The following example shows the output of the command:

```
(Extreme 220) #show version bootloader
Querying Active and Backup Software, please wait ....
Running Version.............................. B1.0.0.5
Active Version............................... B1.0.0.5
Backup Version............................... B1.0.0.2
```

environment temprange

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

Format	`environment temprange min` *-100-100* `max` *-100-100*
Mode	Global Config

Parameter	Definition
min	Sets the minimum allowed temperature for normal operation. The range is between –100°C and 100°C. The default is 0°C.
max	Sets the maximum allowed temperature for normal operation. The range is between –100°C and 100°C. The default is 0°C.

environment trap

Use this command to configure environment status traps.

Format	`environment trap {fan|powersupply|temperature}`
Mode	Global Config

Parameter	Definition
fan	Enables or disables the sending of traps for fan status events. The default is enabled.
powersupply	Enables or disables the sending of traps for power supply status events. The default is enabled.
temperature	Enables or disables the sending of traps for temperature status events. The default is enabled.

show environment

This command displays information about system disk space and usage.

Format	`show environment`
Mode	Privileged EXEC

The command output shows the following values:

Column	Meaning
Unit	The system unit number.
Total Space	The total amount of disk space on the system, in KB.
Free Space	The amount of available disk space on the system, in KB.
Used Space	The amount of disk space in use on the system, in KB.
Utilization	The amount of disk space in use on the system, as a percentage of total disk space.

The following shows an example of the command output:

```
Unit   Total space (KB)   Free space (KB)   Used space (KB)   Utilization (%)
----   ----------------   ---------------   ---------------   ---------------
1               126,976            85,976            41,000               32
```

Logging Commands

This section describes the commands used to configure system logging, and to view logs and the logging settings.

logging buffered

This command enables logging to an in-memory log.

Default	Disabled; critical when enabled
Format	`logging buffered`
Mode	Global Config

no logging buffered

This command disables logging to in-memory log.

Format	`no logging buffered`
Mode	Global Config

logging buffered wrap

This command enables wrapping of in-memory logging when the log file reaches full capacity. Otherwise when the log file reaches full capacity, logging stops.

Default	enabled
Format	`logging buffered wrap`
Mode	Privileged EXEC

no logging buffered wrap

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

Format	`no logging buffered wrap`
Mode	Privileged EXEC

logging cli-command

This command enables the CLI command logging feature, which enables the 200 Series software to log all CLI commands issued on the system. The commands are stored in a persistent log. Use the `show logging persistent` command to display the stored history of CLI commands.

Default	enabled
Format	`logging cli-command`
Mode	Global Config

no logging cli-command

This command disables the CLI command logging feature.

Format	`no logging cli-command`
Mode	Global Config

logging console

This command enables logging to the console.

Possible severity levels for logging messages are as follows. (You can enter either the word or the corresponding numeral.)

- **emergency (0)**: The device is unusable.
- **alert (1)**: Action must be taken immediately.
- **critical (2)**: The device is experiencing primary system failures.
- **error (3)**: The device is experiencing non-urgent failures.
- **warning (4)**: The device is experiencing conditions that could lead to system errors if no action is taken.
- **notice (5)**: The device is experiencing normal but significant conditions.
- **info (6)**: The device is providing non-critical information.
- **debug (7)**: The device is providing debug-level information.

Default	Disabled; critical (2) when enabled
Format	`logging console` *`[severity-level]`*
Mode	Global Config

no logging console

This command disables logging to the console.

Format	`no logging console`
Mode	Global Config

logging host

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

Default	• port: 514 (for UDP) and 6514 (for TLS) • authentication mode: anonymous • certificate index: 0 • level: critical (2)
Format	`logging host {`*`hostaddress`*`|`*`hostname`*`} addresstype tls`*`[anon|x509name] certificate-index {port severity-level}`*
Mode	Global Config

Parameter	Description
hostaddress | *hostname*	The IP address of the logging host.
address-type	The type of address being passed: DNS or IPv4.
tls	Enables TLS security for the host.
anon | *x509name*	The type of authentication mode: anonymous or x509name.
certificate-index	The certificate number to be used for authentication. The valid range is 0–8. Index 0 is used to the default file.
port	A port number from 1 to 65535.
severity-level	The severity level of logging messages. The possible values are as follows. (You can enter either the word or the corresponding numeral.) • **emergency (0)**: The device is unusable. • **alert (1)**: Action must be taken immediately. • **critical (2)**: The device is experiencing primary system failures. • **error (3)**: The device is experiencing non-urgent failures. • **warning (4)**: The device is experiencing conditions that could lead to system errors if no action is taken. • **notice (5)**: The device is experiencing normal but significant conditions. • **info (6)**: The device is providing non-critical information. • **debug (7)**: The device is providing debug-level information.

The following example shows how the command could be entered.

```
(Extreme 220) (Config) # logging host google.com dns 214
(Extreme 220) (Config) # logging host 10.130.64.88 ipv4 214 6
(Extreme 220) (Config) # logging host 5.5.5.5 ipv4 tls anon 6514 debug
(Extreme 220) (Config) # logging host 5.5.5.5 ipv4 tls x509name 3 6514 debug
```

logging host reconfigure

This command enables logging host reconfiguration.

Format	`logging host reconfigure` *hostindex*
Mode	Global Config

Parameter	Description
hostindex	Enter the Logging Host Index for which to change the IP address.

logging host remove

This command disables logging to host. See show logging hosts on page 174 for a list of host indexes.

Format	`logging host remove` *hostindex*
Mode	Global Config

logging protocol

Use this command to configure the logging protocol version number as 0 or 1. RFC 3164 uses version 0 and RFC 5424 uses version 1.

Default	The default is version 0 (RFC 3164).
Format	`logging protocol {0|1}`
Mode	Global Config

logging syslog

This command enables syslog logging. Use the optional facility parameter to set the default facility used in syslog messages for components that do not have an internally assigned facility. The facility value can be one of the following keywords: kernel, user, mail, system, security, syslog, lpr, nntp, uucp, cron, auth, ftp, ntp, audit, alert, clock, local0, local1, local2, local3, local4, local5, local6, local7. The default facility is local7.

Default	Disabled
Format	`logging syslog [facility` *`facility`*`]`
Mode	Global Config

no logging syslog

This command disables syslog logging.

Format	`no logging syslog [facility]`
Mode	Global Config

logging syslog port

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

Default	Disabled
Format	`logging syslog port` *`portid`*
Mode	Global Config

no logging syslog port

This command disables syslog logging.

Format	`no logging syslog port`
Mode	Global Config

logging syslog source-interface

This command configures the syslog source-interface (source IP address) for syslog 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 specific switch. If a source-interface is not specified, the primary IP address of the originating (outbound) interface is used as the source address.

Format	`logging syslog source-interface {`*`unit/slot/port`*`|{`**`loopback`** *`loopback-id`*`}|{`**`vlan`** *`vlan-id`*`}}`
Mode	Global Config

Parameter	Description
unit/slot/port	VLAN or port-based routing interface.
loopback-id	Configures the loopback interface to use as the source IP address. The range of the loopback ID is 0 to 7.
vlan-id	Configures the VLAN interface to use as the source IP address. The range of the VLAN ID is 1 to 4093.

The following example shows how the command could be entered.

```
(config)#logging syslog source-interface loopback 0
(config)#logging syslog source-interface tunnel 0
(config)#logging syslog source-interface 0/4/1
(config)#logging syslog source-interface 1/0/1
```

no logging syslog source-interface

This command disables syslog logging.

Format	`no logging syslog`
Mode	Global Config

show logging

This command displays logging configuration information.

Format	`show logging`
Mode	Privileged EXEC

Column	Meaning
Logging Client Local Port	Port on the collector/relay to which syslog messages are sent.
Logging Client Source Interface	Shows the configured syslog source-interface (source IP address).
CLI Command Logging	Shows whether CLI Command logging is enabled.
Logging Protocol	The logging protocol version number.

Column	Meaning
	• 0: RFC 3164 • 1: RFC 5424
Console Logging	Shows whether console logging is enabled.
Console Logging Severity Filter	The minimum severity to log to the console log. Messages with an equal or lower numerical severity are logged.
Buffered Logging	Shows whether buffered logging is enabled.
Persistent Logging	Shows whether persistent logging is enabled.
Persistent Logging Severity Filter	The minimum severity at which the logging entries are retained after a system reboot.
Syslog Logging	Shows whether syslog logging is enabled.
Syslog Logging Facility	Shows the value set for the facility in syslog messages.
Log Messages Received	Number of messages received by the log process. This includes messages that are dropped or ignored.
Log Messages Dropped	Number of messages that could not be processed due to error or lack of resources.
Log Messages Relayed	Number of messages sent to the collector/relay.

The following example shows CLI display output for the command.

```
(Extreme 220) (Routing) #show logging
Logging Client Local Port           : 514
Logging Client USB File Name        :
Logging Client Source Interface     : (not configured)
CLI Command Logging                 : disabled
Console Logging                     : enabled
Console Logging Severity Filter     : error
Buffered Logging                    : enabled
Buffered Logging Severity Filter    : info
Persistent Logging                  : disabled
Persistent Logging Severity Filter  : alert
Syslog Logging                      : disabled
Syslog Logging Facility             : local7
Log Messages Received               : 229
Log Messages Dropped                : 0
Log Messages Relayed                : 0
```

show logging buffered

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

Format	`show logging buffered`
Mode	Privileged EXEC

Column	Meaning
Buffered (In-Memory) Logging	Shows whether the In-Memory log is enabled or disabled.
Buffered Logging Wrapping Behavior	The behavior of the In-Memory log when faced with a log full situation.
Buffered Log Count	The count of valid entries in the buffered log.

show logging hosts

This command displays all configured logging hosts. Use the pipe (|) character to display the output filter options.

Format	`show logging hosts`
Mode	Privileged EXEC

Column	Meaning
Host Index	(Used for deleting hosts.)
IP Address / Hostname	IP address or hostname of the logging host.
Severity Level	The message severity level: • **emergency (0)**: The device is unusable. • **alert (1)**: Action must be taken immediately. • **critical (2)**: The device is experiencing primary system failures. • **error (3)**: The device is experiencing non-urgent failures. • **warning (4)**: The device is experiencing conditions that could lead to system errors if no action is taken. • **notice (5)**: The device is experiencing normal but significant conditions. • **info (6)**: The device is providing non-critical information. • **debug (7)**: The device is providing debug-level information.
Port	The server port number, which is the port on the local host from which syslog messages are sent.
Status	Status field provides the current status of snmp row status. (Active, Not in Service, Not Ready).
Mode	The type of security: UDP or TLS.
Auth	The type of authentication mode: anonymous or x509name.
Cert #	The certificate number to be used for authentication. The valid range is 0–8. Index 0 is used to the default file.

The following example shows CLI display output for the command.

```
(Extreme 220) (Routing) #show logging hosts
Index  IP Address/Hostname  Severity   Port   Status    Mode
-----  -------------------- ---------- ------ --------- -----
1      1.1.1.17             critical   514    Active    udp
2      10.130.191.90        debug      10514  Active    tls
3      5.5.5.5              debug      333    Active    tls
Auth     Cert#
-------- -----
x509name 6
x509name 4
```

show logging persistent

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

Format	`show logging persistent [log-files]`
Mode	Privileged EXEC

Column	Meaning
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.

The following example shows CLI display output for the command.

```
(Extreme 220) (Switching)#show logging persistent
Persistent Logging                        : disabled
Persistent Log Count                        : 0
(Extreme 220) (Switching)#show logging persistent log-files
Persistent Log Files:
slog0.txt
slog1.txt
slog2.txt
olog0.txt
olog1.txt
olog2.txt
```

show logging traplogs

This command displays *SNMP (Simple Network Management Protocol)* trap events and statistics.

Format	`show logging traplogs`
Mode	Privileged EXEC

Column	Meaning
Number of Traps Since Last Reset	The number of traps since the last boot.
Trap Log Capacity	The number of traps the system can retain.
Number of Traps Since Log Last Viewed	The number of new traps since the command was last executed.
Log	The log number.
System Time Up	How long the system had been running at the time the trap was sent.
Trap	The text of the trap message.

clear logging buffered

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

Format	`clear logging buffered`
Mode	Privileged EXEC

Email Alerting and Mail Server Commands

logging email

This command enables email alerting and sets the lowest severity level for which log messages are emailed. If you specify a severity level, log messages at or above this severity level, but below the urgent severity level, are emailed in a non-urgent manner by collecting them together until the log time expires.

Possible severity levels for logging messages are as follows. (You can enter either the word or the corresponding numeral.)

- **emergency (0)**: The device is unusable.
- **alert (1)**: Action must be taken immediately.
- **critical (2)**: The device is experiencing primary system failures.
- **error (3)**: The device is experiencing non-urgent failures.
- **warning (4)**: The device is experiencing conditions that could lead to system errors if no action is taken.
- **notice (5)**: The device is experiencing normal but significant conditions.
- **info (6)**: The device is providing non-critical information.
- **debug (7)**: The device is providing debug-level information.

Default	Disabled; when enabled, log messages at or above severity Warning (4) are emailed
Format	`logging email [severity-level]`
Mode	Global Config

no logging email

This command disables email alerting.

Format	`no logging email`
Mode	Global Config

logging email urgent

This command sets the lowest severity level at which log messages are emailed immediately in a single email message.

Possible severity levels for logging messages are as follows. (You can enter either the word or the corresponding numeral.)

- **emergency (0)**: The device is unusable.
- **alert (1)**: Action must be taken immediately.
- **critical (2)**: The device is experiencing primary system failures.
- **error (3)**: The device is experiencing non-urgent failures.

- **warning (4)**: The device is experiencing conditions that could lead to system errors if no action is taken.
- **notice (5)**: The device is experiencing normal but significant conditions.
- **info (6)**: The device is providing non-critical information.
- **debug (7)**: The device is providing debug-level information.

Default	Alert (1) and emergency (0) messages are sent immediately.
Format	`logging email urgent {`*`severity-level`* `| none}`
Mode	Global Config

no logging email urgent

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

Format	`no logging email urgent`
Mode	Global Config

logging email message-type to-addr

This command configures the email address to which messages are sent. The message types supported are urgent, non-urgent, and both. For each supported severity level, multiple email addresses can be configured. The to-email-addr variable is a standard email address, for example admin@yourcompany.com.

Format	`logging email message-type {urgent |non-urgent |both} to-addr` *`to-email-addr`*
Mode	Global Config

no logging email message-type to-addr

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

Format	`no logging email message-type {urgent |non-urgent |both} to-addr` *`to-email-addr`*
Mode	Global Config

logging email from-addr

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

Format	`logging email from-addr` *`from-email-addr`*
Mode	Global Config

no logging email from-addr

This command removes the configured email source address.

Format	`no logging email from-addr` *`from-email-addr`*
Mode	Global Config

logging email message-type subject

This command configures the subject line of the email for the specified type.

Default	For urgent messages: Urgent Log Messages For non-urgent messages: Non-Urgent Log Messages
Format	`logging email message-type {urgent |non-urgent |both} subject subject`
Mode	Global Config

no logging email message-type subject

This command removes the configured email subject for the specified message type and restores it to the default email subject.

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

logging email logtime

This command configures how frequently non-urgent email messages are sent. Non-urgent messages are collected and sent in a batch email at the specified interval. The valid range is every 30–1440 minutes.

Default	30 minutes
Format	`logging email logtime minutes`
Mode	Global Config

no logging email logtime

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

Format	`no logging email logtime`
Mode	Global Config

logging traps

This command sets the severity at which *SNMP* traps are logged and sent in an email.

Possible severity levels for logging messages are as follows. (You can enter either the word or the corresponding numeral.)

- **emergency (0)**: The device is unusable.
- **alert (1)**: Action must be taken immediately.
- **critical (2)**: The device is experiencing primary system failures.
- **error (3)**: The device is experiencing non-urgent failures.
- **warning (4)**: The device is experiencing conditions that could lead to system errors if no action is taken.
- **notice (5)**: The device is experiencing normal but significant conditions.
- **info (6)**: The device is providing non-critical information.
- **debug (7)**: The device is providing debug-level information.

Default	Info (6) messages and higher are logged.
Format	`logging traps` *`severity-level`*
Mode	Global Config

no logging traps

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

Format	`no logging traps`
Mode	Global Config

logging email test message-type

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

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

show logging email config

This command displays information about the email alert configuration.

Format	`show logging email config`
Mode	Privileged EXEC

Column	Meaning
Email Alert Logging	The administrative status of the feature: enabled or disabled

Column	Meaning
Email Alert From Address	The email address of the sender (the switch).
Email Alert Urgent Severity Level	The lowest severity level that is considered urgent. Messages of this type are sent immediately.
Email Alert Non Urgent Severity Level	The lowest severity level that is considered non-urgent. Messages of this type, up to the urgent level, are collected and sent in a batch email. Log messages that are less severe are not sent in an email message at all.
Email Alert Trap Severity Level	The lowest severity level at which traps are logged.
Email Alert Notification Period	The amount of time to wait between non-urgent messages.
Email Alert To Address Table	The configured email recipients.
Email Alert Subject Table	The subject lines included in urgent (Type 1) and non-urgent (Type 2) messages.
For Msg Type urgent, subject is	The configured email subject for sending urgent messages.
For Msg Type non-urgent, subject is	The configured email subject for sending non-urgent messages.

show logging email statistics

This command displays email alerting statistics.

Format	`show logging email statistics`
Mode	Privileged EXEC

Column	Meaning
Email Alert Operation Status	The operational status of the email alerting feature.
No of Email Failures	The number of email messages that have attempted to be sent but were unsuccessful.
No of Email Sent	The number of email messages that were sent from the switch since the counter was cleared.
Time Since Last Email Sent	The amount of time that has passed since the last email was sent from the switch.

clear logging email statistics

This command resets the email alerting statistics.

Format	`clear logging email statistics`
Mode	Privileged EXEC

mail-server

This command configures the SMTP server to which the switch sends email alert messages and changes the mode to Mail Server Configuration mode. The server address can be in the IPv4, IPv6, or DNS name format.

Format	`mail-server {ip-address | ipv6-address | hostname}`
Mode	Global Config

no mail-server

This command removes the specified SMTP server from the configuration.

Format	`no mail-server {ip-address | ipv6-address | hostname}`
Mode	Global Config

security

This command sets the email alerting security protocol by enabling the switch to use TLS authentication with the SMTP Server. If the TLS mode is enabled on the switch but the SMTP sever does not support TLS mode, no email is sent to the SMTP server.

Default	none
Format	`security {tlsv1 | none}`
Mode	Mail Server Config

port

This command configures the TCP port to use for communication with the SMTP server. The recommended port for TLSv1 is 465, and for no security the recommended port is 25. However, any nonstandard port in the range 1 to 65535 is allowed.

Default	25
Format	`port {465 | 25 | 1-65535}`
Mode	Mail Server Config

username (Mail Server Config)

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

Default	admin
Format	`username name`
Mode	Mail Server Config

password

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

Default	admin
Format	`password password`
Mode	Mail Server Config

show mail-server config

This command displays information about the email alert configuration.

Format	`show mail-server {ip-address | hostname | all} config`
Mode	Privileged EXEC

Column	Meaning
No of mail servers configured	The number of SMTP servers configured on the switch.
Email Alert Mail Server Address	The IPv4/IPv6 address or DNS hostname of the configured SMTP server.
Email Alert Mail Server Port	The TCP port the switch uses to send email to the SMTP server
Email Alert Security Protocol	The security protocol (TLS or none) the switch uses to authenticate with the SMTP server.
Email Alert Username	The username the switch uses to authenticate with the SMTP server.
Email Alert Password	The password the switch uses to authenticate with the SMTP server.

System Utility and Clear Commands

This section describes the commands used to help troubleshoot connectivity issues and to restore various configurations to their factory defaults.

traceroute

Use this command to discover the routes that IPv4 or IPv6 packets actually take when traveling to their destination through the network on a hop-by-hop basis. Traceroute continues to provide a synchronous response when initiated from the CLI.

You can 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 (Internet Control Message Protocol)* error messages back to the source address from each hop along the forward path to the destination. By specifying the source address,you can determine where along the forward path there is no route back to the source address. Note that this is only useful if the route from source to destination and destination to source is symmetric. It would be common, for example, to send a traceroute from an edge router to a target higher in the network using a source address from a host subnet on the edge router. This would test reachability from within the network back to hosts attached to the edge router. 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, you can specify the source as an IPv4 address, IPv6 address, a virtual router, or as a routing interface. When the source is specified as a routing interface, the traceroute is sent using the primary

IPv4 address on the source interface. With *SNMP*, the source must be specified as an address. The source cannot be specified in the web UI.

200 Series will not accept an incoming packet, such as a traceroute response, that arrives on a routing interface if the packet's destination address is on one of the out-of-band management interfaces (service port or network port). Similarly, 200 Series will not accept a packet that arrives on a management interface if the packet's destination is an address on a routing interface. Thus, it would be futile to send a traceroute on a management interface using a routing interface address as source, or to send a traceroute on a routing interface using a management interface as source. When sending a traceroute on a routing interface, the source must be that routing interface or another routing interface. When sending a traceroute on a management interface, the source must be on that management interface. For this reason, you cannot specify the source as a management interface or management interface address. When sending a traceroute on a management interface, you should not specify a source address, but instead let the system select the source address from the outgoing interface.

Default	• count: 3 probes • interval: 3 seconds • size: 0 bytes • port: 33434 • maxTtl: 30 hops • maxFail: 5 probes • initTtl: 1 hop
Format	`traceroute` *`ip-address`* `| [ipv6] {`*`ipv6-address`* `|` *`hostname`*`}} [initTtl` *`initTtl`*`] [maxTtl` *`maxTtl`*`] [maxFail` *`maxFail`*`] [interval` *`interval`*`] [count` *`count`*`] [port` *`port`*`] [size` *`size`*`] [source {`*`ip-address`* `| |` *`ipv6-address`* `|` *`unit/slot/port`*`}]`
Mode	Privileged EXEC

Using the following options, 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
`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. Range is 0 to 255.
`maxTtl`	Use **maxTtle** to specify the maximum TTL. Range is 1 to 255.
`maxFail`	Use **maxFail** to terminate the traceroute after failing to receive a response for this number of consecutive probes. Range is 0 to 255.

Parameter	Description
interval	Use the optional **interval** parameter to specify the time between probes, in seconds. If a response is not received within this interval, then traceroute considers that probe a failure (printing *) and sends the next probe. If traceroute does receive a response to a probe within this interval, then it sends the next probe immediately. Range is 1 to 60 seconds.
count	Use the optional **count** parameter to specify the number of probes to send for each TTL value. Range is 1 to 10 probes.
port	Use the optional **port** parameter to specify destination UDP port of the probe. This should be an unused port on the remote destination system. Range is 1 to 65535.
size	Use the optional **size** parameter to specify the size, in bytes, of the payload of the Echo Requests sent. Range is 0 to 65507 bytes.
source	Use the optional source parameter to specify the source IP address or interface for the traceroute.

The following are examples show the CLI output for this command.

Successful execution of`traceroute`:

```
(Extreme 220) (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
```

```
(Extreme 220) (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
The above command can also be execute with the optional ipv6 parameter as follows:
(Extreme 220) (Routing) # traceroute ipv6 2001::2 initTtl 1 maxTtl 4 maxFail 0 interval 1
count 3 port 33434 size 43
```

Unsuccessful execution of`traceroute`:

```
(Extreme 220) (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
```

```
(Extreme 220) (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
```

clear config

This command resets the configuration to the factory defaults without powering off the switch. When you issue this command, you are prompted to confirm that the reset should proceed. When you respond with `y`, the switch's current configuration is reset to the factory default values. The switch is not rebooted.

Format	`clear config`
Mode	Privileged EXEC

clear counters

This command clears the statistics for a specified unit/slot/port, for all the ports, or for an interface on a VALN based on the argument, including the loop protection counters.

Format	`clear counters {`*`unit/slot/port`*` | all | vlan `*`id`*`}`
Mode	Privileged EXEC

clear igmpsnooping

This command clears the tables managed by the *IGMP (Internet Group Management Protocol)* Snooping function and attempts to delete these entries from the Multicast Forwarding Database.

Format	`clear igmpsnooping`
Mode	Privileged EXEC

clear ip access-list counters

This command clears the counters of the specified IP *ACL (Access Control List)* and IP ACL rule.

Format	`clear ip access-list counters `*`acl-ID | acl-name rule-id`*
Mode	Privileged EXEC

clear ipv6 access-list counters

This command clears the counters of the specified IP *ACL* and IP ACL rule.

Format	`clear ipv6 access-list counters `*`acl-name rule-id`*
Mode	Privileged EXEC

clear mac access-list counters

This command clears the counters of the specified MAC *ACL* and MAC ACL rule.

Format	`clear mac access-list counters` *`acl-name rule-id`*
Mode	Privileged EXEC

clear pass

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

Format	`clear pass`
Mode	Privileged EXEC

clear traplog

This command clears the trap log.

Format	`clear traplog`
Mode	Privileged EXEC

clear vlan

This command resets VLAN configuration parameters to the factory defaults. When the VLAN configuration is reset to the factory defaults, there are some scenarios regarding GVRP and MVRP that happen due to this:

1 Static VLANs are deleted.

2 GVRP is restored to the factory default as a result of handling the VLAN RESTORE NOTIFY event. Since GVRP is disabled by default, this means that GVRP should be disabled and all of its dynamic VLANs should be deleted.

3 MVRP is restored to the factory default as a result of handling the VLAN RESTORE NOTIFY event. Since MVRP is enabled by default, this means that any VLANs already created by MVRP are unaffected. However, for customer platforms where MVRP is disabled by default, then the MVRP behavior should match GVRP. That is, MVRP is disabled and the MVRP VLANs are deleted.

Format	`clear vlan`
Mode	Privileged EXEC

logout

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

Note
Save configuration changes before logging out.

Format	`logout`
Modes	• Privileged EXEC • User EXEC

ping

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

Note
For information about the `ping` command for IPv6 hosts, see ping ipv6 on page 579.

Default	• The default count is 1. • The default interval is 3 seconds. • The default size is 0 bytes.
Format	`ping {`*`ip-address`*`| `*`hostname`*`	{`**`ipv6`**` {interface {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/slot/port	vlan `*`1-4093`*`	serviceport	network}] [`**`outgoing-interface`**` {unit/slot/port	vlan 1-4093	serviceport	network}]`
Modes	• Privileged EXEC • User EXEC

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

Parameter	Description
`ip-address`	IPv4 or IPv6 addresses to ping.
`count`	Use the count parameter to specify the number of ping packets (*ICMP* Echo requests) that are sent to the destination address specified by the *`ip-address`* field. The range for *`count`* is 1 to 15 requests.
`interval`	Use the interval parameter to specify the time between Echo Requests, in seconds. Range is 1 to 60 seconds.
`size`	Use the size parameter to specify the size, in bytes, of the payload of the Echo Requests sent. Range is 0 to 65507 bytes.

Parameter	Description
source	Use the *source* parameter to specify the source IP/IPv6 address or interface to use when sending the Echo requests packets.
hostname	Use the *hostname* parameter to resolve to an IPv4 or IPv6 address. The ipv6 keyword is specified to resolve the hostname to IPv6 address. The IPv4 address is resolved if no keyword is specified.
ipv6	The optional keyword *ipv6* can be used before the *ipv6-address* or *hostname* argument. Using the *ipv6* optional keyword before *hostname* tries to resolve it directly to the IPv6 address. Also used for pinging a link-local IPv6 address.
interface	Use the interface keyword to ping a link-local IPv6 address over an interface.
link-local-address	The link-local IPv6 address to ping over an interface.
outgoing-interface	Use the outgoing-interface parameter to specify the outgoing interface for multicast IP/IPv6 ping.

The following are examples of the CLI command.

IPv4 ping success:

```
(Extreme 220) (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
```

IPv6 ping success:

```
(Extreme 220) (Routing) #ping 2001::1
 Pinging 2001::1 with 64 bytes of data:
Send count=3, Receive count=3 from 2001::1
Average round trip time = 3.00 ms
```

IPv4 ping failure:

In Case of Unreachable Destination:

```
(Extreme 220) (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:

```
(Extreme 220) (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
```

IPv6 ping failure:

```
(Extreme 220) (Routing) #ping ipv6 2001::4
 Pinging 2001::4 with 64 bytes of data:
Send count=3, Receive count=0 from 2001::4
Average round trip time = 0.00 ms
```

quit

This command closes the current Telnet connection or resets the current serial connection. The system asks you whether to save configuration changes before quitting.

Format	`quit`
Modes	• Privileged EXEC • User EXEC

reload

This command reboots the switch without powering it off. This 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 reboot should proceed. The LEDs on the switch indicate a successful reboot.

Format	`reload [configuration [`*`scriptname`*`]]`
Mode	Privileged EXEC

Parameter	Description
`configuration`	Gracefully reloads the configuration. If no configuration file is specified, the startup-config file is loaded.
`scriptname`	The configuration file to load. The scriptname must include the extension.

copy

The `copy` command uploads and downloads files to and from the switch. You can also use the `copy` command to manage the dual images (active and backup) on the file system. Upload and download files from a server using FTP, TFTP, Xmodem, Ymodem, or Zmodem. SFTP and SCP are available as additional transfer methods if the software package supports secure management. If FTP is used, a password is required.

Format	`copy` *`source destination`* `{`*`verify`*` | `*`noverify`*`}`
Mode	Privileged EXEC

Replace the source and destination parameters with the options in Table 11 on page 190. For the URL source or destination, use one of the following values:

`{xmodem | tftp://`*`ipaddr`*`|`*`hostname`*` | `*`ip6address`*`|`*`hostname/filepath/filename`*` [noval]| sftp| scp://`*`username@ipaddr`*` | `*`ipv6address/filepath/filename`*` | ftp://`*`user@ipaddress`*` | `*`hostname/filepath/filename`*`}`

verify | noverify is only available if the image/configuration verify options feature is enabled (see file verify on page 193). verify specifies that digital signature verification will be performed for the specified downloaded image or configuration file. noverify specifies that no verification will be performed.

The keyword **ias-users** supports the downloading of the IAS user database file. When the IAS users file is downloaded, the switch IAS user's database is replaced with the users and its attributes available in the downloaded file. In the command `copy url ias-users`, for *`url`* one of the following is used for IAS users file:

tftp:// {ipaddr | hostname} | {ipv6address | hostname/filepath/filename}
sftp | scp://username@ipaddress/filepath/filename

Note
The maximum length for the file path is 160 characters, and the maximum length for the file name is 31 characters.

For FTP, TFTP, SFTP and SCP, the ipaddr|hostname parameter is the IP address or host name of the server, filepath is the path to the file, and filename is the name of the file you want to upload or download. For SFTP and SCP, the username parameter is the username for logging into the remote server via SSH.

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

For platforms that include stacking, use the optional [unit unit id] parameter (when available) to specify the stack member to use as the source for the item to copy. If no unit is specified, the item is copied from the stack master.

To copy OpenFlow SSL certificates to the switch using TFTP or XMODEM, using only the following options pertinent to the OpenFlow SSL certificates.

Format	`copy {mode | file} nvram:{openflow-ssl-ca-cert | openflow-ssl-cert | openflow-ssl-priv-key}`
Mode	Privileged EXEC

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

Table 11: Copy Parameters

Source	Destination	Description
nvram:application: *`sourcefilename`*	*`url`*	Filename of source application file.
nvram:backup-config	nvram:startup-config	Copies the backup configuration to the startup configuration.
nvram:clibanner	*`url`*	Copies the CLI banner to a server.

Table 11: Copy Parameters (continued)

Source	Destination	Description
nvram: core-dump [unit *unit id*]	One of the following: tftp://*ipaddress* | *hostname/filepath/filename* ftp://*ipaddress* | *hostname/filepath/filename* scp://*ipaddress* | *hostname/filepath/filename* sftp://*ipaddress* | *hostname/filepath/filename*	Uploads the core dump file on the local system to an external TFTP/FTP/SCP/SFTP server.
nvram:cpupktcapture.pcap [unit *unit id*]	*url*	Uploads CPU packets capture file.
nvram:crash-log	url	Copies the crash log to a server.
nvram:errorlog	*url*	Copies the error log file to a server.
nvram:factory-defaults	*url*	Uploads factory defaults file.
nvram:fastpath.cfg	*url*	Uploads the binary config file to a server.
nvram:log	*url*	Copies the log file to a server.
nvram:operational-log [unit *unit id*]	url	Copies the operational log file to a server.
nvram:script *scriptname*	*url*	Copies a specified configuration script file to a server.
nvram:startup-config	nvram:backup-config	Copies the startup configuration to the backup configuration.
nvram:startup-config	*url*	Copies the startup configuration to a server.
nvram:startup-log [unit *unit id*]	url	Uploads the startup log file.
nvram: tech-support [unit *unit id*]	url	Uploads the system and configuration information for technical support.
nvram:traplog	*url*	Copies the trap log file to a server.
system:running-config	nvram:startup-config	Saves the running configuration to NVRAM.
system:running-config	nvram:factory-defaults	Saves the running configuration to NVRAM to the **factory-defaults** file.
system:image	url	Saves the system image to a server.
tftp:// *ipaddress/filename*	system:packet.pcap	Copies a PCAP file into RAM. The PCAP file is used to inject packets into the silicon for tracing the packets.
url	nvram:application *destfilename*	Destination file name for the application file.
url	nvram:ca-root *index*	Downloads the CA certificate file to the /mnt/fastpath directory and uses the index number name the downloaded file to CA*index*.pem.

Table 11: Copy Parameters (continued)

Source	Destination	Description
url	nvram:clibanner	Downloads the CLI banner to the system.
url	nvram:client-key *index*	Downloads the client key file to the /mnt/fastpath directory and uses the index number name the downloaded file to CA*index*.key.
url	nvram:client-ssl-cert *1–8*	Downloads the client certificate to the /mnt/fastpath directory and uses the index number to name the downloaded file to CA*index*.pem.
url	nvram:fastpath.cfg	Downloads the binary config file to the system.
url	nvram:publickey-config	Downloads the Public Key for Configuration Script validation.
url	nvram:publickey-image	Downloads Public Key for Image validation.
url	nvram:script *destfilename*	Downloads a configuration script file to the system. During the download of a configuration script, the copy command validates the script. In case of any error, the command lists all the lines at the end of the validation process and prompts you to confirm before copying the script file.
url	nvram:script *destfilename* noval	When you use this option, the copy command will not validate the downloaded script file. An example of this command follows:
(Extreme 220) (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 on page 50.
url	nvram:sshkey-rsa1	Downloads an SSH key file.
url	nvram:sshkey-rsa2	Downloads an SSH key file.
url	nvram:sslpem-dhweak	Downloads an HTTP secure-server certificate.
url	nvram:sslpem-dhstrong	Downloads an HTTP secure-server certificate.
url	nvram:sslpem-root	Downloads an HTTP secure-server certificate. For more information, see Hypertext Transfer Protocol Commands on page 54.
url	nvram:sslpem-server	Downloads an HTTP secure-server certificate.
url	nvram:startup-config	Downloads the startup configuration file to the system.
url	ias-users	Downloads an IAS users database file to the system. When the IAS users file is downloaded, the switch IAS user's database is replaced with the users and their attributes available in the downloaded file.
url	nvram:tech-support-cmds	Downloads the file containing list of commands to be displayed using the **`show tech-support`** command.
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.

Table 11: Copy Parameters (continued)

Source	Destination	Description
{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.

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

```
(Extreme 220) (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.
(Extreme 220) (Routing) #
```

file verify

This command enables digital signature verification while an image and/or configuration file is downloaded to the switch.

Format	`file verify {all | image | none | script}`
Mode	Global Config

Parameter	Description
all	Verifies the digital signature of both image and configuration files.
image	Verifies the digital signature of image files only.
none	Disables digital signature verification for both images and configuration files.
script	Verifies the digital signature of configuration files.

no file verify

Resets the configured digital signature verification value to the factory default value.

Format	`no file verify`
Mode	Global Config

write memory

Use this command to save running configuration changes to NVRAM so that the changes you make will persist across a reboot. This command is the same as copy system:running-config nvram:startup-config. Use the confirm keyword to directly save the configuration to NVRAM without prompting for a confirmation.

Format	`write memory [confirm]`
Mode	Privileged EXEC

Power Over Ethernet Commands

This section describes the commands used to configure and monitor *PoE (Power over Ethernet)*. PoE allows IP telephones, wireless LAN access points, and other appliances to receive power as well as data over existing LAN cabling without modifying the existing Ethernet infrastructure. PoE is only available on switches that contain a PoE controller.

PoE implements the PoE+ specification (IEEE 802.3at) for power sourcing equipment (PSE). IEEE 802.3at allows power to be supplied to Class 4 PD devices that require power greater than 15.4 Watts and up to 34.2 Watts. This allows the PoE+ enabled network switches and routers to be used for deployment with devices that require more power than the 802.3AF specification allows. PoE+ 802.3at is compatible with 802.1AF.

Flexible Power Management

PoE provides power management that supports power reservation, power prioritization, and power limiting. The operator can assign a priority to each PoE port. When the power budget of the PoE switch has been exhausted, the higher priority ports are given preference over the lower priority ports. Lower priority ports are forcibly stopped to supply power in order to provide power to higher priority ports.

The static power management feature allows operators to reserve a guaranteed amount of power for a PoE port. This is useful for powering up devices which draw variable amounts of power and provide them an assured power range within which to operate. Class-based power management allocates power at class limits as opposed to user-defined limits.

In the Dynamic Power management feature, power is not reserved for a given port at any point of time. The power available with the PoE switch is calculated by subtracting the instantaneous power drawn by all the ports from the maximum available power. Thus, more ports can be powered at the same time. This feature is useful to efficiently power up more devices when the available power with the PoE switch is limited.

PoE also provides a global usage threshold feature in order to limit the PoE switch from reaching an overload condition. The operator can specify the limit as a percentage of the maximum power.

Note
PoE commands are only applicable to copper ports.

poe

Use this command to enable/disable *PoE* admin mode. If enabled, all ports (Interface Config mode) or the selected port (Interface Config mode) are capable of delivering power to a PD (powered device). If disabled, none of the ports can deliver power to a PD.

Note
PoE admin mode does not impact the functionality of the Ethernet port itself; disabling admin mode only turns off the capability to deliver power.

Default	Enabled
Format	`poe`
Mode	• Global Configuration • Interface Configuration

poe detection

Use this command to set the detection mode. Detection mode is used to set the type of devices that will be allowed for powering up. You can configure the *PoE* controller to detect only IEEE standard devices or pre-IEEE legacy devices (which were pre-standard). Use the no form of the command to bring detection mode back to the default setting of auto.

Default	auto
Format	`poe detection {auto | ieee | pre-ieee}`
Mode	Interface Configuration

Parameter	Description
auto	Detects both standard and non-standard devices.
ieee	Detects IEEE standard devices.
pre-ieee	Detects legacy devices.

poe high-power

Use this command to enable high power mode for all ports in all units (Global Configuration) or for a specific unit (Interface Configuration mode). In high power mode, the switch negotiates the power budget with the powered device (PD). A PoE port can deliver up to 32 W of power in dot3at mode.

Default	Disabled
Format	`poe high-power {dot3at | legacy | pre-dot3at}`
Mode	• Global Configuration • Interface Configuration

Parameter	Description
dot3at	High power device with *LLDP (Link Layer Discovery Protocol)* support.
legacy	Powered device with a high-inrush current.
pre-dot3at	Powered device without LLDP support.

no poe high-power

Disables high power mode.

Format	`no poe high-power`
Mode	• Global Configuration • Interface Configuration

poe power limit

Use this command to configure the type of power limit for all ports in all units (Global Configuration) or a specified port (Interface Configuration).

Default	User-defined value
Format	`poe power limit {none| value | class-based}`
Mode	• Global Configuration • Interface Configuration

Parameter	Description
none	There is no power limit.
value	A user-defined power limit from 3000 mW to 32000 mW power per port.
class-based	The power limit is class-based.

no power power limit

Use this command to set the power limit type to the default.

Default	User-defined value
Format	`no poe power limit`
Mode	• Global Configuration • Interface Configuration

poe power management

Use this command to set up the power management type.

Default	Dynamic
Format	`poe power management {`*`unit/slot/port`*` | all} {dynamic | static}`
Mode	Global Configuration

Parameter	Description
`unit`	Configures power management for an individual port.
`all`	Configures power management for all ports.
`dynamic`	Power management is done by the PoE controller and the maximum power for a port is not reserved for each port.
`static`	Power management is done by the PoE controller and maximum power for a port is reserved.

no poe power management

Use this command to set the management mode to the default.

Format	`no poe power management`
Mode	Global Configuration

poe priority

Use this command to configure the port priority level for the delivery of power to an attached device. The switch may not be able to supply power to all connected devices, so the port priority is used to determine which ports will supply power if adequate power capacity is not available for all enabled ports. For ports that have the same priority level the lower-numbered port has higher priority.

For a system delivering peak power to a certain number of devices, if a new device is attached to a high-priority port, power to a low-priority port is shut down and the new device is powered up.

Default	Low
Format	`poe priority { Crit | Hig | Low | Medium}`
Mode	Interface Configuration

no poe priority

Use this command to return the port priority level to the default value.

Default	Low
Format	`no poe priority`
Mode	• Global Configuration • Interface Configuration

poe reset

Use this command to reset all ports.

Default	Disabled
Format	`poe reset`
Mode	Global Configuration

poe traps

Use this command to enable/disable traps that indicate changes in the *PoE* status for the port.

Default	Enable
Format	`poe traps`
Mode	Global Configuration

poe usagethreshold

Use this command to configure the system power usage threshold level at which a trap is generated. The threshold is configured as a percentage of the total available power.

Default	90%
Format	`poe usagethreshold {unit | all} 1-99`
Mode	Global Configuration

Parameter	Description
`unit`	Sets the threshold for the unit.
`all`	Sets the threshold for all units.
1-99	The power threshold at which a trap is generated. The range is 1-99%.

no poe usagethreshold

Use this command to set the threshold to the default value.

Format	`no poe usagethreshold`
Mode	Global Configuration

show poe

Use this command to display the current PoE configuration and status information for all ports.

Format	`show poe`
Mode	Privileged EXEC

Column	Meaning
Firmware Version	The firmware version on the controller. This value cannot be changed or upgraded.
PSE Main Operational Status	The operational status of the PSE.
Total Power Available	The total power budget.
Threshold Power	The total power minus the guard band. If usage goes above this value, new ports are not powered up.
Total Power Consumed	Total power delivered by all ports.
Usage Threshold	User-configured threshold, used for Guard band calculation.
Power Management Mode	The current power management mode: Dynamic or Static.
Traps	Whether *PoE* traps are enabled or disabled.

The following example shows CLI display output for the command.

```
(Extreme 220) #show poe
Firmware Version.............................. 1.3.0.7
PSE Main Operational Status................... OFF
Total Power Available......................... 900 Watts
Threshold Power............................... 459 W
Total Power Consumed.......................... 0
Usage Threshold............................... 90
Power Management Mode......................... Dynamic
Traps......................................... Enable
```

show poe port configuration

Use this command to display PoE port configuration information for individual ports or all ports.

Format	`show poe port configuration { all | unit/slot/port }`
Mode	Privileged EXEC

```
(Extreme 220) #show poe port configuration 0/1
         Admin              Power   Power Limit    High Power      Detection       Timer
Schedule
Intf    Mode   Priority Limit      Type          Mode                Type
                         (mW)
------ ------- -------- ------ -------------- ------------- ---------------------
----------------
0/1    Enable     Low   60000   User Defined    UPOE              auto
None
```

show poe port info

Use this command to display *PoE* port information.

Format	`show poe port info { all | unit/slot/port }`
Mode	Privileged EXEC

```
(Extreme 220) #show poe port info all
        High     Max                          Output  Output
Intf    Power    Power     Class    Power     Current Voltage      Status             Fault
                  (mW)                (mW)      (mA)    (V)                          Status
------ ------- -------- -------- --------  ------- -------  -----------------
-----------------
2/0/1    Yes    32000    Unknown  0          0       0       Disabled           No Error
2/0/2    Yes    32000    Unknown  0          0       0       Disabled           No Error
2/0/3    Yes    32000    Unknown  0          0       0       Disabled           No Error
2/0/4    Yes    32000    Unknown  0          0       0       Disabled           No Error
2/0/5    Yes    32000    Unknown  0          0       0       Disabled           No Error
2/0/6    Yes    32000    Unknown  0          0       0       Disabled           No Error
2/0/7    Yes    32000    Unknown  0          0       0       Disabled           No Error
2/0/8    Yes    32000    Unknown  0          0       0       Disabled           No Error
2/0/9    Yes    32000    Unknown  0          0       0       Disabled           No Error
2/0/10   Yes    32000    Unknown  0          0       0       Disabled           No Error
2/0/11   Yes    32000    Unknown  0          0       0       Disabled           No Error
2/0/12   Yes    32000    Unknown  0          0       0       Disabled           No Error
2/0/13   Yes    32000    Unknown  0          0       0       Disabled           No Error
2/0/14   Yes    32000    Unknown  0          0       0       Disabled           No Error
2/0/15   Yes    32000    Unknown  0          0       0       Disabled           No Error
2/0/16   Yes    32000    Unknown  0          0       0       Disabled           No Error
2/0/17   Yes    32000    Unknown  0          0       0       Disabled           No Error
2/0/18   Yes    32000    Unknown  0          0       0       Disabled           No Error
```

Simple Network Time Protocol Commands

This section describes the commands used to automatically configure the system time and date by using *SNTP*.

sntp broadcast client poll-interval

This command sets the poll interval for *SNTP* broadcast clients in seconds as a power of two where poll-interval can be a value from 6 to 10.

Default	6
Format	`sntp broadcast client poll-interval` *`poll-interval`*
Mode	Global Config

no sntp broadcast client poll-interval

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

Format	`no sntp broadcast client poll-interval`
Mode	Global Config

sntp client mode

This command enables *SNTP* client mode and may set the mode to either broadcast or unicast.

Default	Disabled
Format	`sntp client mode [broadcast | unicast]`
Mode	Global Config

no sntp client mode

This command disables *SNTP* client mode.

Format	`no sntp client mode`
Mode	Global Config

sntp client port

This command sets the *SNTP* client port ID to 0, 123 or a value between 1025 and 65535. The default value is 0, which means that the SNTP port is not configured by the user. In the default case, the actual client port value used in SNTP packets is assigned by the underlying OS.

Default	0
Format	`sntp client port portid`
Mode	Global Config

no sntp client port

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

Format	`no sntp client port`
Mode	Global Config

sntp unicast client poll-interval

This command sets the poll interval for *SNTP* unicast clients in seconds as a power of two where poll-interval can be a value from 6 to 10.

Default	6
Format	`sntp unicast client poll-interval poll-interval`
Mode	Global Config

no sntp unicast client poll-interval

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

Format	`no sntp unicast client poll-interval`
Mode	Global Config

sntp unicast client poll-timeout

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

Default	5
Format	`sntp unicast client poll-timeout` *`poll-timeout`*
Mode	Global Config

no sntp unicast client poll-timeout

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

Format	`no sntp unicast client poll-timeout`
Mode	Global Config

sntp unicast client poll-retry

This command will set the poll retry for *SNTP* unicast clients to a value from 0 to 10.

Default	1
Format	`sntp unicast client poll-retry` *`poll-retry`*
Mode	Global Config

no sntp unicast client poll-retry

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

Format	`no sntp unicast client poll-retry`
Mode	Global Config

sntp server

This command configures an *SNTP* server (a maximum of three). The server address can be either an IPv4 address or an IPv6 address. The optional priority can be a value of 1-3, the version a value of 1-4, and the port id a value of 1-65535.

Format	`sntp server {`*`ipaddress`* `|` *`ipv6address`* `|` *`hostname`*`} [`*`priority`* `[`*`version`* `[`*`portid`*`]]]`
Mode	Global Config

no sntp server

This command deletes an server from the configured *SNTP* servers.

Format	`no sntp server remove {ipaddress | ipv6address | hostname}`
Mode	Global Config

sntp source-interface

Use this command to specify the physical or logical interface to use as the source interface (source IP address) for *SNTP* unicast server configuration. If configured, the address of source Interface is used for all SNTP communications between the SNTP server and the SNTP client. 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 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 SNTP client falls back to its default behavior.

Format	`sntp source-interface {unit/slot/port |` **`loopback`** *`loopback-id`* `|` **`vlan`***`vlan-id`* `|` **`network`** `|` **`serviceport`**`}`
Mode	Global Config

Parameter	Description
unit/slot/port	The unit identifier assigned to the switch.
loopback *loopback-id*	Configures the loopback interface. The range of the loopback ID is 0 to 7.
vlan *vlan-id*	Configures the VLAN interface to use as the source IP address. The range of the VLAN ID is 1 to 4093.
network	Uses the network source IP as the source address.
serviceport	Uses the management port source IP as the source address.

no sntp source-interface

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

Format	`no sntp source-interface`
Mode	Global Config

show sntp

This command is used to display *SNTP* settings and status.

Format	`show sntp`
Mode	Privileged EXEC

Column	Meaning
Last Update Time	Time of last clock update.
Last Unicast Attempt Time	Time of last transmit query (in unicast mode).
Last Attempt Status	Status of the last SNTP request (in unicast mode) or unsolicited message (in broadcast mode).
Broadcast Count	Current number of unsolicited broadcast messages that have been received and processed by the SNTP client since last reboot.

show sntp client

This command is used to display *SNTP* client settings.

Format	`show sntp client`
Mode	Privileged EXEC

Column	Meaning
Client Supported Modes	Supported SNTP Modes (Broadcast or 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 to port 123; if the client is in unicast mode, it binds to the port assigned by the underlying OS.
Client Mode	Configured SNTP Client Mode.

show sntp server

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

Format	`show sntp server`
Mode	Privileged EXEC

Column	Meaning
Server Host Address	IP address or hostname of configured SNTP Server.
Server Type	Address type of server (IPv4, IPv6, or DNS).
Server Stratum	Claimed stratum of the server for the last received valid packet.
Server Reference ID	Reference clock identifier of the server for the last received valid packet.
Server Mode	SNTP Server mode.
Server Maximum Entries	Total number of SNTP Servers allowed.
Server Current Entries	Total number of SNTP configured.

For each configured server:

Column	Meaning
IP Address / Hostname	IP address or hostname of configured SNTP Server.
Address Type	Address Type of configured SNTP server (IPv4, IPv6, or DNS).
Priority	IP priority type of the configured server.
Version	SNTP Version number of the server. The protocol version used to query the server in unicast mode.
Port	Server Port Number.
Last Attempt Time	Last server attempt time for the specified server.
Last Update Status	Last server attempt status for the server.
Total Unicast Requests	Number of requests to the server.
Failed Unicast Requests	Number of failed requests from server.

show sntp source-interface

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

Format	`show sntp source-interface`
Mode	Privileged EXEC

Column	Meaning
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	The IP address of the interface configured as the SNTP client source interface.

The following example shows CLI display output for the command.

```
(Extreme 220) (Routing) #show sntp source-interface
SNTP Client Source Interface.................. (not configured)
(Extreme 220) (Routing) #
```

Time Zone Commands

Use the Time Zone commands to configure system time and date, Time Zone and Summer Time (that is, Daylight Saving Time). Summer time can be recurring or non-recurring.

clock set

This command sets the system time and date.

Format	`clock set` *`hh:mm:ss`* `clock set` *`mm/dd/yyyy`*
Mode	Global Config

Parameter	Description
hh:mm:ss	Enter the current system time in 24-hour format in hours, minutes, and seconds. The range is hours: 0 to 23, minutes: 0 to 59, seconds: 0 to 59.
mm/dd/yyyy	Enter the current system date the format month, day, year. The range for month is 1 to 12. The range for the day of the month is 1 to 31. The range for year is 2010 to 2079.

The following example shows how the command could be entered.

```
(Extreme 220) (Config) # clock set 03:17:00
(Extreme 220) (Config) # clock set 11/01/2011
```

clock summer-time date

Use the clock summer-time date command to set the summer-time offset to Coordinated Universal Time (UTC). If the optional parameters are not specified, they are read as either 0 or \0, as appropriate.

Format	`clock summer-time date {`*`date month year hh:mm date month year hh:mm`*`}[`**`offset`** *`offset`*`] [`**`zone`***`acronym`*`]`
Mode	Global Config

Parameter	Description
date	Day of the month. Range is 1 to 31.
month	Month. The range is the first three letters by name (for example, Jan).
year	Year. The range is 2000 to 2097.
hh:mm	Time in 24-hour format in hours and minutes. The range is hours: 0 to 23, minutes: 0 to 59.
offset	The number of minutes to add during the summertime. The range is 1 to 1440.
acronym	The acronym for the summer-time to be displayed when summertime is in effect. Up to four characters are allowed.

The following example shows how the command could be entered.

```
(Extreme 220) (Config) # clock summer-time date 1 nov 2011 3:18 2 nov 2011 3:18
(Extreme 220) (Config) # clock summer-time date 1 nov 2011 3:18 2 nov 2011 3:18 offset 120
zone INDA
```

clock summer-time recurring

This command sets the summer-time recurring parameters.

Format	`clock summer-time recurring {`*`week day month hh:mm week day month hh:mm`*`} [`**`offset`** *`offset`*`] [`**`zone`** *`acronym`*`]`
Mode	Global Config

Parameter	Description
EU	The system clock uses the standard recurring summer time settings used in countries in the European Union.
USA	The system clock uses the standard recurring daylight saving time settings used in the United States.
week	Week of the month. The range is 1 to 5, **first**, or **last**.
day	Day of the week. The range is the first three letters by name; sun, for example.
month	Month. The range is the first three letters by name; jan, for example.
hh:mm	Time in 24-hour format in hours and minutes. The range is hours: 0 to 23, minutes: 0 to 59.
offset	The number of minutes to add during the summertime. The range is 1 to 1440.
acronym	The acronym for the summertime to be displayed when summertime is in effect. Up to four characters are allowed.

The following example shows how the command could be entered.

```
(Extreme 220) (Config) # clock summer-time recurring 2 sun nov 3:18 2 mon nov 3:18
(Extreme 220) (Config) # clock summer-time recurring 2 sun nov 3:18 2 mon nov 3:18 offset
120 zone INDA
```

no clock summer-time

This command disables the summer-time settings.

Format	`no clock summer-time`
Mode	Global Config

The following shows an example of the command.

```
(Extreme 220) (Config) # no clock summer-time
```

clock timezone

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

Format	`clock timezone {`*hours*`} [minutes` *minutes*`] [zone` *acronym*`]`
Mode	Global Config

Parameter	Description
hours	Hours difference from UTC. The range is -12 to +13.
minutes	Minutes difference from UTC. The range is 0 to 59.
acronym	The acronym for the time zone. The range is up to four characters.

The following shows an example of the command.

```
(Extreme 220) (Config) # clock timezone 5 minutes 30 zone INDA
```

no clock timezone

Use this command to reset the time zone settings.

Format	`no clock timezone`
Mode	Global Config

show clock

Use this command to display the time and date from the system clock.

Format	`show clock`
Mode	Privileged EXEC

The following examples show CLI display output for the command.

```
(Extreme 220) (Routing) # show clock
15:02:09 (UTC+0:00) Nov 1 2017
No time source
```

```
(Extreme 220) (Routing) # show clock
10:55:40 INDA(UTC+7:30) Nov 1 2017
No time source
```

show clock detail

Use this command to display the detailed system time along with the time zone and the summertime configuration.

Format	`show clock detail`
Mode	Privileged EXEC

The following examples show CLI display output for the command.

```
(Extreme 220) (Routing) # show clock detail
15:05:24 (UTC+0:00) Nov 1 2017
No time source
Time zone:
Acronym not configured
Offset is UTC+0:00
Summertime:
Summer-time is disabled
```

```
(Extreme 220) (Routing) # show clock detail
10:57:57 INDA(UTC+7:30) Nov 1 2017
No time source
 Time zone:
 Acronym is INDA
 Offset is UTC+5:30
 Summertime:
 Acronym is INDA
```

```
Recurring every year
Begins on second Sunday of Nov at 03:18
Ends on second Monday of Nov at 03:18
Offset is 120 minutes
Summer-time is disabled
```

DHCP Server Commands

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

ip dhcp pool

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

Default	None
Format	`ip dhcp pool` *`name`*
Mode	Global Config

no ip dhcp pool

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

Format	`no ip dhcp pool` *`name`*
Mode	Global Config

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
Format	`client-identifier` *`uniqueidentifier`*
Mode	DHCP Pool Config

no client-identifier

This command deletes the client identifier.

Format	`no client-identifier`
Mode	DHCP Pool Config

client-name

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

Default	None
Format	`client-name` *`name`*
Mode	DHCP Pool Config

no client-name

This command removes the client name.

Format	`no client-name`
Mode	DHCP Pool Config

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
Format	`default-router` *`address1 [address2....address8]`*
Mode	DHCP Pool Config

no default-router

This command removes the default router list.

Format	`no default-router`
Mode	DHCP Pool Config

dns-server

This command specifies the IP servers available to a *DHCP* client. Address parameters 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
Format	`dns-server address1 [address2....address8]`
Mode	DHCP Pool Config

no dns-server

This command removes the DNS Server list.

Format	`no dns-server`
Mode	DHCP Pool Config

hardware-address

This command specifies the hardware address of a *DHCP* client.

hardwareaddress is the MAC address of the client's hardware platform, consisting of six bytes in dotted hexadecimal format.

Default	ethernet
Format	`hardware-address hardwareaddress`
Mode	DHCP Pool Config

no hardware-address

This command removes the hardware address of the *DHCP* client.

Format	`no hardware-address`
Mode	DHCP Pool Config

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
Format	`host address [{mask | prefix-length}]`
Mode	DHCP Pool Config

no host

This command removes the IP address of the *DHCP* client.

Format	`no host`
Mode	DHCP Pool Config

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)
Format	`lease [{`*`days`* `[`*`hours`*`] [`*`minutes`*`] | infinite}]`
Mode	DHCP Pool Config

no lease

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

Format	`no lease`
Mode	DHCP Pool Config

network (DHCP Pool Config)

Use 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
Format	`network` *`networknumber`* `[{`*`mask`* `|` *`prefixlength`*`}]`
Mode	DHCP Pool Config

no network

This command removes the subnet number and mask.

Format	`no network`
Mode	*DHCP* Pool Config

bootfile

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

Format	`bootfile` *`filename`*
Mode	DHCP Pool Config

no bootfile

This command deletes the boot image name.

Format	`no bootfile`
Mode	DHCP Pool Config

domain-name

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

Default	None
Format	`domain-name` *`domain`*
Mode	DHCP Pool Config

no domain-name

This command removes the domain name.

Format	`no domain-name`
Mode	DHCP Pool Config

domain-name enable

This command enables the domain name functionality in 200 Series.

Format	`domain-name enable [name` *`name`*`]`
Mode	DHCP Pool Config

no domain-name enable

This command disables the domain name functionality in 200 Series.

Format	`no domain-name enable`
Mode	Global Config

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
Format	`netbios-name-server` *`address`* `[`*`address2...address8`*`]`
Mode	DHCP Pool Config

no netbios-name-server

This command removes the NetBIOS name server list.

Format	`no netbios-name-server`
Mode	DHCP Pool Config

netbios-node-type

The command configures the NetBIOS node type for Microsoft *DHCP* clients. *`type`* Specifies the NetBIOS node type. Valid types are:

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

Default	None
Format	`netbios-node-type` *`type`*
Mode	DHCP Pool Config

no netbios-node-type

This command removes the NetBIOS node Type.

Format	`no netbios-node-type`
Mode	DHCP Pool Config

next-server

This command configures 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
Format	`next-server address`
Mode	DHCP Pool Config

no next-server

This command removes the boot server list.

Format	`no next-server`
Mode	*DHCP* Pool Config

option

The 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, a3:4f:22:0c), or space (for example, a3 4f 22 0c).

Default	None
Format	`option code {ascii string | hex string1 [string2...string8] | ip address1 [address2...address8]}`
Mode	DHCP Pool Config

no option

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

Format	`no option code`
Mode	DHCP Pool Config

ip dhcp excluded-address

This command specifies the IP addresses that a *DHCP* server should not assign to DHCP clients. The *lowaddress* and *highaddress* 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
Format	`ip dhcp excluded-address` *`lowaddress [highaddress]`*
Mode	Global Config

no ip dhcp excluded-address

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

Format	`no ip dhcp excluded-address` *`lowaddress [highaddress]`*
Mode	Global Config

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
Format	`ip dhcp ping packets` *`0,2-10`*
Mode	Global Config

no ip dhcp ping packets

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

Format	`no ip dhcp ping packets`
Mode	Global Config

service dhcp

This command enables the *DHCP* server.

Default	Disabled
Format	`service dhcp`
Mode	Global Config

no service dhcp

This command disables the *DHCP* server.

Format	`no service dhcp`
Mode	Global Config

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	Disabled
Format	`ip dhcp bootp automatic`
Mode	Global Config

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.

Format	`no ip dhcp bootp automatic`
Mode	Global Config

ip dhcp conflict logging

This command enables conflict logging on the *DHCP* server.

Default	Enabled
Format	`ip dhcp conflict logging`
Mode	Global Config

no ip dhcp conflict logging

This command disables conflict logging on the *DHCP* server.

Format	`no ip dhcp conflict logging`
Mode	Global Config

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. The *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.

Format	`clear ip dhcp binding {address | *}`
Mode	Privileged EXEC

clear ip dhcp server statistics

This command clears *DHCP* server statistics counters.

Format	`clear ip dhcp server statistics`
Mode	Privileged EXEC

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
Format	`clear ip dhcp conflict {address | *}`
Mode	Privileged EXEC

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.

Format	`show ip dhcp binding [address]`
Modes	• Privileged EXEC • User EXEC

Column	Meaning
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 manner in which IP address was assigned to the client.

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.

Format	`show ip dhcp global configuration`
Modes	• Privileged EXEC • User EXEC

Column	Meaning
Service DHCP	The status of the DHCP protocol.
Number of Ping Packets	The maximum number of ping packets that will be sent to verify that an IP address ID is not already assigned.
Conflict Logging	Whether conflict logging is enabled or disabled.
BootP Automatic	Whether BootP for dynamic pools is enabled or disabled.

show ip dhcp pool configuration

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

Format	`show ip dhcp pool configuration {`*`name`*` | all}`
Modes	• Privileged EXEC • User EXEC

Column	Meaning
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:

Column	Meaning
Network	The network number and the mask for the DHCP address pool.

The following additional fields are displayed for Manual pool type:

Column	Meaning
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.

show ip dhcp server statistics

This command displays *DHCP* server statistics.

Format	`show ip dhcp server statistics`
Modes	• Privileged EXEC • User EXEC

Column	Meaning
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.
DHCP DISCOVER packets discarded	The number of messages discarded from one or more DHCP Discovers.

Messages Received:

Column	Meaning
DHCP DISCOVER	The number of DHCPDISCOVER messages the server has received.
DHCP REQUEST	The number of DHCPREQUEST messages the server has received.
DHCP DECLINE	The number of DHCPDECLINE messages the server has received.
DHCP RELEASE	The number of DHCPRELEASE messages the server has received.
DHCP INFORM	The number of DHCPINFORM messages the server has received.

Messages Sent:

Column	Meaning
DHCP OFFER	The number of DHCPOFFER messages the server sent.
DHCP ACK	The number of DHCPACK messages the server sent.
DHCP NACK	The number of DHCPNACK messages the server sent.

show ip dhcp conflict

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

Format	`show ip dhcp conflict [ip-address]`
Modes	• Privileged EXEC • User EXEC

Column	Meaning
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.

Column	Meaning
Detection time	The time when the conflict was found.

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 200 Series.

ip domain lookup

Use this command to enable the DNS client.

Default	Enabled
Format	`ip domain lookup`
Mode	Global Config

no ip domain lookup

Use this command to disable the DNS client.

Format	`no ip domain lookup`
Mode	Global Config

ip domain name

Use this command to define a default domain name that 200 Series software uses to complete unqualified host names (names with a domain name). By default, no default domain name is configured in the system. name may not be longer than 255 characters and should not include an initial period. This name should be used only when the default domain name list, configured using the ip domain list command, is empty.

Default	None
Format	`ip domain name` *`name`*
Mode	Global Config

The CLI command ip domain name yahoo.com will configure yahoo.com as a default domain name. For an unqualified hostname xxx, a DNS query is made to find the IP address corresponding to xxx.yahoo.com.

no ip domain name

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

Format	`no ip domain name`
Mode	Global Config

ip domain list

Use this command to define a list of default domain names to complete unqualified names. By default, the list is empty. Each name must be no more than 256 characters, and should not include an initial period. The default domain name, configured using the ip domain name command, is used only when the default domain name list is empty. A maximum of 32 names can be entered in to this list.

Default	None
Format	`ip domain list` *`name`*
Mode	Global Config

no ip domain list

Use this command to delete a name from a list.

Format	`no ip domain list` *`name`*
Mode	Global Config

ip name server

Use this command to configure the available name servers. Up to eight servers can be defined in one command or by using multiple commands. The parameter server-address is a valid IPv4 or IPv6 address of the server. The preference of the servers is determined by the order they were entered.

Format	`ip name-server` *`server-address1`* `[`*`server-address2...server-address8`*`]`
Mode	Global Config

no ip name server

Use this command to remove a name server.

Format	`no ip name-server [`*`server-address1...server-address8`*`]`
Mode	Global Config

ip name source-interface

Use this command to specify the physical or logical interface to use as the DNS client (IP name) source interface (source IP address) for the DNS client management application. If configured, the address of source Interface is used for all DNS communications between the DNS server and the DNS client. 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 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 DNS client falls back to its default behavior.

Format	`sntp source-interface {`*`unit/slot/port`* `|`**`loopback`** *`loopback-id`* `|` **`vlan`***`vlan-id`* `|` **`network`** `|` **`serviceport`**`}`
Mode	Global Config

Parameter	Description
`unit/slot/port`	The unit identifier assigned to the switch.
`loopback` *`loopback-id`*	Configures the loopback interface. The range of the loopback ID is 0 to 7.
`vlan` *`vlan-id`*	Configures the VLAN interface to use as the source IP address. The range of the VLAN ID is 1 to 4093.
`network`	Uses the network source IP as the source address.
`serviceport`	Uses the management port source IP as the source address.

no ip name source-interface

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

Format	`no ip name source-interface`
Mode	Global Config

ip host

Use this command to define static host name-to-address mapping in the host cache. The parameter *`name`* is host name and *`ipaddress`* is the IP address of the host. The host name can include 1–255 alphanumeric characters, periods, hyphens, underscores, and non-consecutive spaces. Hostnames that include one or more space must be enclosed in quotation marks, for example “lab-pc 45”.

Default	None
Format	`ip host` *`name ipaddress`*
Mode	Global Config

no ip host

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

Format	`no ip host` *`name`*
Mode	Global Config

ipv6 host

Use this command to define static host name-to-IPv6 address mapping in the host cache. The parameter *name* is host name and *v6 address* is the IPv6 address of the host. The host name can include 1–255 alphanumeric characters, periods, hyphens, and spaces. Hostnames that include one or more space must be enclosed in quotation marks, for example “lab-pc 45”.

Default	None
Format	`ipv6 host` *`name v6 address`*
Mode	Global Config

no ipv6 host

Use this command to remove the static host name-to-IPv6 address mapping in the host cache.

Format	`no ipv6 host` *`name`*
Mode	Global Config

ip domain retry

Use this command to specify the number of times to retry sending Domain Name System (DNS) queries. The parameter *number* indicates the number of times to retry sending a DNS query to the DNS server. This number ranges from 0 to 100.

Default	2
Format	`ip domain retry` *`number`*
Mode	Global Config

no ip domain retry

Use this command to return to the default.

Format	`no ip domain retry` *`number`*
Mode	Global Config

ip domain timeout

Use this command to specify the amount of time to wait for a response to a DNS query. The parameter *seconds* specifies the time, in seconds, to wait for a response to a DNS query. The range is from 0 to 3600 seconds.

Default	3
Format	`ip domain timeout` *`seconds`*
Mode	Global Config

no ip domain timeout

Use this command to return to the default setting.

Format	`no ip domain timeout` *seconds*
Mode	Global Config

clear host

Use this command to delete entries from the host name-to-address cache. This command clears the entries from the DNS cache maintained by the software. This command clears both IPv4 and IPv6 entries.

Format	`clear host {`*name* `| all}`
Mode	Privileged EXEC

Field	Description
name	A particular host entry to remove. The range is from 1-255 characters.
all	Removes all entries.

show hosts

Use this command to display the default domain name, a list of name server hosts, the static and the cached list of host names and addresses. The parameter *name* ranges from 1-255 characters. This command displays both IPv4 and IPv6 entries.

Format	`show hosts` *[name]*
Mode	• Privileged EXEC • User EXEC

Column	Meaning
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.
DNS Client Source Interface	Shows the configured source interface (source IP address) used for a DNS client. The IP address of the selected interface is used as source IP for all communications with the server.

The following example shows CLI display output for the command.

```
(Extreme 220) # show hosts
Host name..................... Device
Default domain................ gm.com
Default domain list........... yahoo.com, Stanford.edu, rediff.com
Domain Name lookup............ Enabled
Number of retries............. 5
Retry timeout period.......... 1500
Name servers (Preference order)... 176.16.1.18 176.16.1.19
DNS Client Source Interface.......     (not configured)
Configured host name-to-address mapping:
Host                          Addresses
----------------------------- -------------------------------
accounting.gm.com             176.16.8.8
Host                          Total          Elapsed                Type
Addresses
--------------- --------     ------    --------     --------------
www.stanford.edu   72                                    3
IP                     171.64.14.203
```

show ip name source-interface

Use this command to display the configured source interface details used for a DNS client. The IP address of the selected interface is used as source IP for all communications with the server.

Format	`show ip name source-interface`
Mode	Privileged EXEC

IP Address Conflict Commands

The commands in this section help troubleshoot IP address conflicts.

ip address-conflict-detect run

This command triggers the switch to run active address conflict detection by sending gratuitous ARP packets for IPv4 addresses on the switch.

Format	`ip address-conflict-detect run`
Mode	• Global Config • Virtual Router Config

show ip address-conflict

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

Format	`show ip address-conflict`
Modes	Privileged EXEC

Column	Meaning
Address Conflict Detection Status	Identifies whether the switch has detected an address conflict on any IP address.
Last Conflicting IP Address	The IP address that was last detected as conflicting on any interface.
Last Conflicting MAC Address	The MAC address of the conflicting host that was last detected on any interface.
Time Since Conflict Detected	The time in days, hours, minutes, and seconds since the last address conflict was detected.

clear ip address-conflict-detect

This command clears the detected address conflict status information.

Format	`clear ip address-conflict-detect`
Modes	Privileged EXEC

Serviceability Packet Tracing Commands

These commands improve the capability of network engineers to diagnose conditions affecting their 200 Series product.

Caution
The output of “debug” commands can be long and may adversely affect system performance.

capture file | remote | line

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

Format	`capture {file | remote | line}`
Mode	Global Config

Parameter	Description
file	In the capture file mode, the captured packets are stored in a file on NVRAM. The maximum file size defaults to 524288 bytes. The switch can transfer the file to a TFTP server via TFTP, SFTP, SCP via CLI, and *SNMP*. The file is formatted in pcap format, is named cpuPktCapture.pcap, and can be examined using network analyzer tools such as Wireshark or Ethereal. Starting a file capture automatically terminates any remote capture sessions and line capturing. After the packet capture is activated, the capture proceeds until the capture file reaches its maximum size, or until the capture is stopped manually using the CLI command `capture stop`.
remote	In the remote capture mode, the captured packets are redirected in real time to an external PC running the Wireshark tool for Microsoft Windows. A packet capture server runs on the switch side and sends the captured packets via a TCP connection to the Wireshark tool. The remote capture can be enabled or disabled using the CLI. There should be a Windows PC with the Wireshark tool to display the captured file. When using the remote capture mode, the switch does not store any captured data locally on its file system. You can configure the IP port number for connecting Wireshark to the switch. The default port number is 2002. If a firewall is installed between the Wireshark PC and the switch, then these ports must be allowed to pass through the firewall. You must configure the firewall to allow the Wireshark PC to initiate TCP connections to the switch. If the client successfully connects to the switch, the CPU packets are sent to the client PC, then Wireshark receives the packets and displays them. This continues until the session is terminated by either end. Starting a remote capture session automatically terminates the file capture and line capturing.
line	In the capture line mode, the captured packets are saved into the RAM and can be displayed on the CLI. Starting a line capture automatically terminates any remote capture session and capturing into a file. There is a maximum 128 packets of maximum 128 bytes that can be captured and displayed in line mode.

capture remote port

Use this command to configure file capture options. The command is persistent across a reboot cycle. The *id* parameter is a TCP port number from 1024– 49151.

Format	`capture remote port` *id*
Mode	Global Config

capture file size

Use this command to configure file capture options. The command is persistent across a reboot cycle. The *file-size* parameter is the maximum size the pcap file can reach, in Kb. The range is from 2 to 512.

Format	`capture file size` *file-size*
Mode	Global Config

capture line wrap

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

Format	`capture line wrap`
Mode	Global Config

no capture line wrap

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

Format	`no capture line wrap`
Mode	Global Config

show capture packets

Use this command to display packets captured and saved to RAM. It is possible to capture and save into RAM, packets that are received or transmitted through the CPU. A maximum 128 packets can be saved into RAM per capturing session. A maximum 128 bytes per packet can be saved into the RAM. If a packet holds more than 128 bytes, only the first 128 bytes are saved; data more than 128 bytes is skipped and cannot be displayed in the CLI.

Capturing packets is stopped automatically when 128 packets are captured and have not yet been displayed during a capture session. Captured packets are not retained after a reload cycle.

Format	`show capture packets`
Mode	Privileged EXEC

cpu-traffic direction interface

Use this command to associate CPU filters to an interface or list of interfaces. The interfaces can be a physical or logical *LAG*. The statistics counters are updated only for the configured interfaces. The traces can also be obtained for the configured interfaces.

Note

The offset should consider the VLAN tag headers as the packet to the CPU is always a tagged packet.

Default	None
Format	`cpu-traffic direction {tx|rx|both} interface` *`interface-range`*
Mode	Global Config

no cpu-traffic direction interface

Use this command to remove all interfaces from the CPU filters.

Format	`no cpu-traffic direction {tx|rx|both} interface` *`interface-range`*
Mode	Global Config

cpu-traffic direction match cust-filter

Use this command to configure a custom filter. The statistics and/or traces for configured filters are obtained for the packet matching configured data at the specific offset. If the mask is not specified, the default mask is 0xFF.

You can specify three different offsets specified as match conditions. Each time a custom filter is configured, the switch overrides the previous configuration.

Note
The offset should consider the VLAN tag headers because the packet to the CPU is always a tagged packet.

Default	None
Format	`cpu-traffic direction {tx|rx|both} match cust-filter` *`offset1 data1`* `[mask` *`mask1`*`]` *`offset2 data2`* `[mask` *`mask2`*`]` *`offset3 data3`* `[mask` *`mask3`*`]`
Mode	Global Config

Parameter	Description
`offset1` *`offset2`* *`offset3`*	Up to three offsets, using the format *`0xXXXX`* where *`XXXX`* is four hexadecimal digits.
`data1` *`data2`* *`data3`*	The two-byte matching value for the corresponding offset, using the format *`0xXXXX`*.
`mask1` *`mask2`* *`mask3`*	The optional two-byte mask for the corresponding offset, using the format *`0xXXXX`*.

The following shows two examples of this command.

```
cpu-traffic direction both match cust-filter 0x0001 0xaabb mask 0xffff
cpu-traffic direction both match cust-filter 0x0001 0xaabb 0x0081 0xccdd 0x00c1 0xeeff
```

no cpu-traffic direction match cust-filter

Use this command to remove the configured custom filter.

Format	`no cpu-traffic direction {tx|rx|both} match cust-filter offset1 data1 [mask mask1] offset2 data2 [mask mask2] offset3 data3 [mask mask3]`
Mode	Global Config

cpu-traffic direction match srcip

Use this command to configure the source IP address-specific filter. The statistics and/or the traces for configured filters are obtained for the packet matching configured source IP/Mask.

Default	None
Format	`cpu-traffic direction {tx|rx|both} match srcip ipaddress [mask mask]`
Mode	Global Config

no cpu-traffic direction match srcip

Use this command to disable the configured source IP address filter.

Format	`no cpu-traffic direction {tx|rx|both} match srcip ipaddress [mask mask]`
Mode	Global Config

cpu-traffic direction match dstip

Use this command to configure the destination IP address-specific filter. The statistics and/or the traces for configured filters are obtained for the packet matching configured destination IP/Mask.

Default	None
Format	`cpu-traffic direction {tx|rx|both} match dstip ipaddress [mask mask]`
Mode	Global Config

no cpu-traffic direction match dstip

Use this command to disable the configured destination IP address filter.

Format	`no cpu-traffic direction {tx|rx|both} match dstip ipaddress [mask mask]`
Mode	Global Config

cpu-traffic direction match tcp

Use this command to configure the source or destination TCP port-specific filter. The statistics and/or traces for configured filters are obtained for the packet matching configured source/destination TCP port.

Default	None
Format	`cpu-traffic direction {tx|rx|both} match {srctcp|dsttcp} port [mask mask]`
Mode	Global Config

no cpu-traffic direction match tcp

Use this command to remove the configured source/destination TCP port filter.

Format	`no cpu-traffic direction {tx|rx|both} match {srctcp|dsttcp} port [mask mask]`
Mode	Global Config

cpu-traffic direction match udp

Use this command to configure the source or destination UDP port-specific filter. The statistics and/or traces for configured filters are obtained for the packet matching configured source/destination UDP port.

Default	None
Format	`cpu-traffic direction {tx|rx|both} match {srcudp|dstudp} port [mask mask]`
Mode	Global Config

no cpu-traffic direction match udp

Use this command to remove the configured source/destination UDP port filter.

Format	`no cpu-traffic direction {tx|rx|both} match {srcudp|dstudp} port [mask mask]`
Mode	Global Config

cpu-traffic mode

Use this command to configure CPU-traffic mode. The packets in the RX/TX direction are matched when the mode is enabled.

Default	Disabled
Format	`cpu-traffic mode`
Mode	Global Config

no cpu-traffic mode

Use this command to disable CPU-traffic mode.

Format	`no cpu-traffic mode`
Mode	Global Config

cpu-traffic trace

Use this command to configure CPU packet tracing. The packet can be received by multiple components. If the feature is enabled and tracing configured, the packets are traced per the defined filter. If dump-pkt is enabled, the first 64 bytes of the packet are displayed along with the trace statistics.

Default	Disabled
Format	`cpu-traffic trace {dump-pkt}`
Mode	Global Config

no cpu-traffic trace

Use this command to disable CPU packet tracing and dump-pkt (if configured).

Format	`no cpu-traffic trace {dump-pkt}`
Mode	Global Config

show cpu-traffic

Use this command to display the current configuration parameters.

Default	None
Format	`show cpu-traffic`
Mode	Privileged EXEC

```
(Extreme 220) (Routing) #show cpu-traffic
Admin Mode..................................... Disable
Packet Trace................................... Disable
Packet Dump.................................... Disable
Direction TX:
Filter Options................................. N/A
Interface...................................... N/A
```

```
Src TCP parameters.............................. 0 0
Dst TCP parameters.............................. 0 0
Src UDP parameters.............................. 0 0
Dst UDP parameters.............................. 0 0
Src IP parameters............................... 0.0.0.0 0.0.0.0
Dst IP parameters............................... 0.0.0.0 0.0.0.0
Src MAC parameters.............................. 00:00:00:00:00:00 00:00:00:00:00:00
Dst MAC parameters.............................. 00:00:00:00:00:00 00:00:00:00:00:00
Custom filter parameters1....................... Offset=0x0 Value=0x0 Mask=0x0
Custom filter parameters2....................... Offset=0x0 Value=0x0 Mask=0x0
Custom filter parameters3....................... Offset=0x0 Value=0x0 Mask=0x0
Direction RX:
Filter Options.................................. N/A
Interface....................................... N/A
Src TCP parameters.............................. 0 0
Dst TCP parameters.............................. 0 0
Src UDP parameters.............................. 0 0
Dst UDP parameters.............................. 0 0
Src IP parameters............................... 0.0.0.0 0.0.0.0
Dst IP parameters............................... 0.0.0.0 0.0.0.0
Src MAC parameters.............................. 00:00:00:00:00:00 00:00:00:00:00:00
Dst MAC parameters.............................. 00:00:00:00:00:00 00:00:00:00:00:00
Custom filter parameters1....................... Offset=0x0 Value=0x0 Mask=0x0
Custom filter parameters2....................... Offset=0x0 Value=0x0 Mask=0x0
Custom filter parameters3....................... Offset=0x0 Value=0x0 Mask=0x0
```

show cpu-traffic interface

Use this command to display interface statistics for configured filters. The statistics can be displayed for a specific filter (for example, stp, udld, arp etc). If no filter is specified, statistics are displayed for all configured filters. Similarly, source/destination IP, TCP, UDP or MAC along with custom filter can be used as command option to get statistics.

Default	None
Format	`show cpu-traffic interface {all | unit/slot/port | cpu } filter`
Mode	Privileged EXEC

show cpu-traffic summary

Use this command to display summary statistics for configured filters for all interfaces.

Default	None
Format	`show cpu-traffic summary`
Mode	Privileged EXEC

```
(Extreme 220) (Routing) #show cpu-traffic summary
Filter       Received   Transmitted
------------ ---------- -----------
STP          0          0
LACPDU       0          0
ARP          0          0
UDLD         0          0
```

```
LLDP          0           0
IP            0           0
OSPF          0           0
BGP           0           0
DHCP          0           0
BCAST         0           0
MCAST         0           0
UCAST         0           0
SRCIP         0           0
DSTIP         0           0
SRCMAC        0           0
DSTMAC        0           0
CUSTOM        0           0
SRCTCP        0           0
DSTTCP        0           0
SRCUDP        0           0
```

show cpu-traffic trace

Use this command to display traced information. The trace information can be displayed either for all available packets or for specific filter (for example, stp, udld, arp etc). Similarly, source/destination IP or MAC along with custom filter can be used as command option to get specific traces from history. If enabled, packet dump information is displayed along with packet trace statistics. By default, packet dump buffer size is set to store first 64 bytes of packet.

Default	None
Format	`show cpu-traffic trace` *`filter`*
Mode	Privileged EXEC

```
(Extreme 220) (Routing) #show cpu-traffic summary
Packet #1: IP; DHCP; UCAST; SRCMAC=00:10:10:10:10:10;
<08:06:10> Sysnet received in sysNetNotifyPduReceive()
<08:06:10> Packet delivered to IP via ipMapRecvIP()
<08:06:10> Freed
0000 00 10 18 82 18 b3 00 10 10 10 10 10 81 00 00 01    ................
0010 08 00 45 10 01 21 00 00 00 00 40 11 79 bd 00 00    ..E..!....@.y...
0020 00 00 ff ff ff ff 00 44 00 43 01 0d 48 10 03 01    .......D.C..H...
0030 06 00 18 85 4a 83 00 00 80 00 00 00 00 00 00 00    ....J...........
```

clear cpu-traffic

Use this command to clear cpu-traffic statistics or trace information on all interfaces.

Default	None
Format	`clear cpu-traffic {counters | traces}`
Mode	Global Config

exception protocol

Use this command to specify the protocol used to store the core dump file.

Note
This command is only available on selected Linux-based platforms.

Default	None
Format	`exception protocol {nfs | tftp | ftp | local | usb | none}`
Mode	Global Config

no exception protocol

Use this command to reset the exception protocol configuration to its factory default value.

Note
This command is only available on Linux-based platforms.

Default	None
Format	`no exception protocol`
Mode	Global Config

exception dump tftp-server

Use this command to configure the IP address of a remote TFTP server in order to dump core files to an external server.

Note
This command is only available on selected Linux-based platforms.

Default	None
Format	`exception dump tftp-server {`*`ip-address`*`}`
Mode	Global Config

no exception dump tftp-server

Use this command to reset the exception dump remote server configuration to its factory default value.

Note
This command is only available on selected Linux-based platforms.

Default	None
Format	`no exception dump tftp-server`
Mode	Global Config

exception dump nfs

Use this command to configure an NFS mount point in order to dump core file to the NFS file system.

Note
This command is only available on selected Linux-based platforms.

Default	None
Format	`exception dump nfs` *`ip-address/dir`*
Mode	Global Config

no exception dump nfs

Use this command to reset the exception dump NFS mount point configuration to its factory default value.

Note
This command is only available on selected Linux-based platforms.

Default	None
Format	`no exception dump nfs`
Mode	Global Config

exception dump filepath

Use this command to configure a file-path to dump core file to a TFTP or FTP server, NFS mount or USB device subdirectory.

Note
This command is only available on selected Linux-based platforms.

Default	None
Format	`exception dump filepath` *`dir`*
Mode	Global Config

no exception dump filepath

Use this command to reset the exception dump filepath configuration to its factory default value.

Note
This command is only available on selected Linux-based platforms.

Default	None
Format	`exception dump filepath`
Mode	Global Config

exception core-file

Use this command to configure a prefix for a core-file name. The core file name is generated with the prefix as follows:

If hostname is selected:

file-name-prefix_hostname_Time_Stamp.bin

If hostname is not selected:

file-name-prefix_MAC_Address_Time_Stamp.bin

If hostname is configured the core file name takes the hostname, otherwise the core-file names uses the MAC address when generating a core dump file. The prefix length is 15 characters.

Note
This command is only available on selected Linux-based platforms.

Default	Core
Format	`exception core-file {`*`file-name-prefix`*` | [hostname] | [time-stamp]}`
Mode	Global Config

no exception core-file

Use this command to reset the exception core file prefix configuration to its factory default value. The hostname and time-stamp are disabled.

Note
This command is only available on selected Linux-based platforms.

Default	Core
Format	`no exception core-file`
Mode	Global Config

exception switch-chip-register

This command enables or disables the switch-chip-register dump in case of an exception. The switch-chip-register dump is taken only for a master unit and not for member units.

Note
This command is only available on selected Linux-based platforms.

Default	Disabled
Format	`exception switch-chip-register {enable | disable}`
Mode	Global Config

exception dump ftp-server

This command configures the IP address of remote FTP server to dump core files to an external server. If the username and password are not configured, the switch uses anonymous FTP. (The FTP server should be configured to accept anonymous FTP.)

Default	None
Format	`exception dump ftp-server` *`ip-address`* `[{username` *`user-name`* `password` *`password`*`}]`
Mode	Global Config

no exception dump ftp-server

This command resets exception dump remote FTP server configuration to its factory default value. This command also resets the FTP username and password to empty string.

Default	None
Format	`no exception dump ftp-server`
Mode	Global Config

exception dump compression

This command enables compression mode.

Default	Enabled
Format	`exception dump compression`
Mode	Global Config

no exception dump compression

This command disables compression mode.

Default	None
Format	`no exception compression`
Mode	Global Config

exception dump stack-ip-address protocol

This command configures protocol (dhcp or static) to be used to configure service port when a unit has crashed. If configured as dhcp then the unit gets the IP address from dhcp server available in the network.

Default	dhcp
Format	`exception dump stack-ip-address protocol {dhcp | static}`
Mode	Global Config

no exception dump stack-ip-address protocol

This command resets stack IP protocol configuration (dhcp or static) to its default value.

Default	None
Format	`no exception dump stack-ip-address protocol`
Mode	Global Config

exception dump stack-ip-address add

This command adds static IP address to be assigned to individual unit's service port in the stack when the switch has crashed. This IP address is used to perform the core dump.

Default	None
Format	`exception dump stack-ip-address add` *`ip-address netmask`* `[`*`gateway`*`]`
Mode	Global Config

exception dump stack-ip-address remove

This command removes stack IP address configuration. If this IP address is assigned to any unit in the stack then this IP is removed from the unit.

Default	None
Format	`exception dump stack-ip-address remove` *`ip-address netmask`*
Mode	Global Config

show exception

Use this command to display the configuration parameters for generating a core dump file.

Note
This command is only available on selected Linux-based platforms.

Default	None
Format	`show exception`
Mode	Privileged EXEC

The following shows an example of this command.

```
show exception
Coredump file name                core
Coredump filename uses hostname   False
Coredump filename uses time-stamp TRUE
TFTP Server Address               TFTP server configuration
FTP Server IP                     FTP server configuration
FTP user name                     FTP user name
FTP password                      FTP password
NFS Mount point                   NFS mount point configuration
File path                         Remote file path
Core File name prefix             Core file prefix configuration.
Hostname                                Core file name contains hostname if enabled.
Timestamp                         Core file name contains timestamp if enabled.
Switch Chip Register Dump         Switch chip register dump configuration
Compression mode                  TRUE/FALSE
Active network port                   0/28
Stack IP Address Protocol         DHCP/Static
Stack IP Address                  List of IP addresses configured
```

show exception core-dump-file

This command displays core dump files existing on the local file system.

Default	None
Format	`show exception core-dump-file`
Mode	Privileged EXEC, Config Mode

show exception log

This command displays core dump traces on the local file system.

Default	None
Format	`show exception log [previous]`
Mode	Privileged EXEC, Config Mode

logging persistent

Use this command to configure the persistent logging for the switch.

Possible severity levels for logging messages are as follows. (You can enter either the word or the corresponding numeral.)

- **emergency (0)**: The device is unusable.
- **alert (1)**: Action must be taken immediately.
- **critical (2)**: The device is experiencing primary system failures.
- **error (3)**: The device is experiencing non-urgent failures.
- **warning (4)**: The device is experiencing conditions that could lead to system errors if no action is taken.
- **notice (5)**: The device is experiencing normal but significant conditions.
- **info (6)**: The device is providing non-critical information.
- **debug (7)**: The device is providing debug-level information.

Default	Disabled
Format	`logging persistent` *`severity-level`*
Mode	Global Config

no logging persistent

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

Format	`no logging persistent`
Mode	Global Config

mbuf

Use this command to configure memory buffer (MBUF) threshold limits and generate notifications when MBUF limits have been reached.

Format	`mbuf {`*`falling-threshold`* `|` *`rising-threshold`* `|` *`severity`*`}`
Mode	Global Config

Field	Description
`rising-threshold`	The percentage of the memory buffer resources that, when exceeded for the configured rising interval, triggers a notification. The range is 1 to 100. The default is 0 (disabled).
`falling-threshold`	The percentage of memory buffer resources that, when usage falls below this level for the configured interval, triggers a notification. The range is 1 to 100. The default is 0 (disabled).
`severity`	The severity level at which Mbuf logs messages. The range is 1 to 7. The default is 5 (L7_LOG_SEVERITY_NOTICE).

show mbuf

Use this command to display the memory buffer (MBUF) Utilization Monitoring parameters.

Format	`show mbuf`
Mode	Privileged EXEC

Field	Description
Rising Threshold	The percentage of the memory buffer resources that, when exceeded for the configured rising interval, triggers a notification. The range is 1 to 100. The default is 0 (disabled).
Falling Threshold	The percentage of memory buffer resources that, when usage falls below this level for the configured interval, triggers a notification. The range is 1 to 100. The default is 0 (disabled).
Severity	The severity level, from 1 to 7.

show mbuf total

Use this command to display memory buffer (MBUF) information.

Format	`show mbuf total`
Mode	Privileged EXEC

Column	Meaning
Mbufs Total	Total number of message buffers in the system.
Mbufs Free	Number of message buffers currently available.
Mbufs Rx Used	Number of message buffers currently in use.
Total Rx Norm Alloc Attempts	Number of times the system tried to allocate a message buffer allocation of class RX Norm.
Total Rx Mid2 Alloc Attempts	Number of times the system tried to allocate a message buffer allocation of class RX Mid2.
Total Rx Mid1 Alloc Attempts	Number of times the system tried to allocate a message buffer allocation of class RX Mid1.
Total Rx Mid0 Alloc Attempts	Number of times the system tried to allocate a message buffer allocation of class RX Mid0.
Total Rx High Alloc Attempts	Number of times the system tried to allocate a message buffer allocation of class RX High.
Total Tx Alloc Attempts	Number of times the system tried to allocate a message buffer allocation of class TX.
Total Rx Norm Alloc Failures	Number of message buffer allocation failures for RX Norm class of message buffer.
Total Rx Mid2 Alloc Failures	Number of message buffer allocation failures for RX Mid2 class of message buffer.
Total Rx Mid1 Alloc Failures	Number of message buffer allocation failures for RX Mid1 class of message buffer.
Total Rx Mid0 Alloc Failures	Number of message buffer allocation failures for RX Mid0 class of message buffer.

Column	Meaning
Total Rx High Alloc Failures	Number of message buffer allocation failures for RX High class of message buffer.
Total Tx Alloc Failures	Number of message buffer allocation failures for TX class of message buffer.

show msg-queue

Use this command to display the message queues.

Default	None
Format	`show msg-queue`
Mode	Privileged EXEC mode

Support Mode Commands

Support mode is hidden and available when the `techsupport enable` command is executed. techsupport mode is disabled by default. Configurations related to support mode are shown in the `show tech-support` command. They can be persisted by using the command save in support mode. Support configurations are stored in a separate binary config file, which cannot be uploaded or downloaded.

techsupport enable

Use this command to allow access to Support mode.

Default	Disabled
Format	`techsupport enable`
Mode	Privileged EXEC

console

Use this command to enable the display of support debug for this session.

Default	Disabled
Format	`console`
Mode	Support

save

Use this command to save the trace configuration to non-volatile storage.

Format	`save`
Mode	Support

snapshot bgp

Use the snapshot bgp command in Support mode to dump a set of BGP debug information to capture the current state of BGP.

Format	`snapshot bgp`
Mode	Support mode

snapshot ospf

Use this command in Support mode to dump a set of OSPF debug information to capture the current state of OSPF. The output is written to the console and can be extensive

Format	`snapshot ospf`
Mode	Support mode

snapshot routing

Use this command in Support mode to dump a set of routing debug information to capture the current state of routing on the switch. The output is written to the console and can be extensive.

Format	`snapshot routing`
Mode	Support

snapshot multicast

Use this command in Support mode to dump a set of IP multicast debug information to capture the current state of multicast on the switch. The output is written to the console and can be extensive.

Format	`snapshot multicast`
Mode	Support

snapshot system

Use this command in Support mode to dump a set of system debug information to capture the current state of the device. The output is written to the console and can be extensive.

Format	`snapshot multicast`
Mode	Support

snapshot vpc

Use this command to dump a set of *MLAG (Multi-switch Link Aggregation Group)* debug information to capture the current state of MLAG. The output is written to the console and can be extensive.

Format	`snapshot vpc`
Mode	Support

telnetd

Use this command in Support mode to start or stop the Telnet daemon on the switch.

Format	`telnetd {start | stop}`
Mode	Support

Cable Test Command

The cable test feature enables you to determine the cable connection status on a selected port.

Note

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.

cablestatus

This command returns the status of the specified port.

Format	`cablestatus` *`unit/slot/port`*
Mode	Privileged EXEC

Column	Meaning
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.

Column	Meaning
	• **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.

sFlow Commands

sFlow is the standard for monitoring high-speed switched and routed networks. sFlow technology is built into network equipment and gives complete visibility into network activity, enabling effective management and control of network resources.

sflow receiver

Use this command to configure the sFlow collector parameters (owner string, receiver timeout, max datagram size, IP address, and port).

Format	`sflow receiver rcvr_idx {owner` *`owner-string`* `timeout` *`rcvr_timeout`* `| max datagram` *`size`* `| ip` *`ip`* `| port` *`port`*`}`
Mode	Global Config

Parameter	Description
owner-string	The identity string for the receiver, the entity making use of this sFlowRcvrTable entry. The range is 127 characters. The default is a null string. The empty string indicates that the entry is currently unclaimed and the receiver configuration is reset to the default values. An entity wishing to claim an sFlowRcvrTable entry must ensure that the entry is unclaimed before trying to claim it. The entry is claimed by setting the owner string to a non-null value. The entry must be claimed before assigning a receiver to a sampler or poller.
rcvr_timeout	The time, in seconds, remaining before the sampler or poller is released and stops sending samples to receiver. A management entity wanting to maintain control of the sampler is responsible for setting a new value before the old one expires. The allowed range is 0-2147483647 seconds. The default is zero (0).
size	The maximum number of data bytes that can be sent in a single sample datagram. The management entity should set this value to avoid fragmentation of the sFlow datagrams. The allowed range is 200 to 9116). The default is 1400.
ip	The sFlow receiver IP address. If set to 0.0.0.0, no sFlow datagrams will be sent. The default is 0.0.0.0.
port	The destination Layer4 UDP port for sFlow datagrams. The range is 1-65535. The default is 6343.

no sflow receiver

Use this command to set the sflow collector parameters back to the defaults.

Format	`no sflow receiver indx {ip` *`ip-address`* `| maxdatagram` *`size`* `| owner` *`string`* `timeout` *`interval`* `| port` *`14-port`*`}`
Mode	Global Config

sflow receiver owner timeout

Use this command to configure a receiver as a timeout entry. As the sFlow receiver is configured as a timeout entry, information related to sampler and pollers are also shown in the running-config and are retained after reboot.

If a receiver is configured with a specific value, these configurations will not be shown in running-config. Samplers and pollers information related to this receiver will also not be shown in running-config.

Format	`sflow receiver` *`index`* `owner` *`owner-string`* `timeout`
Mode	Global Config

Parameter	Description
`index`	Receiver index identifier. The range is 1 to 8.
`owner-string`	The owner name corresponds to the receiver name. The identity string for the receiver, the entity making use of this sFlowRcvrTable entry. The range is 127 characters. The default is a null string. The empty string indicates that the entry is currently unclaimed and the receiver configuration is reset to the default values. An entity wishing to claim an sFlowRcvrTable entry must ensure that the entry is unclaimed before trying to claim it. The entry is claimed by setting the owner string to a non-null value. The entry must be claimed before assigning a receiver to a sampler or poller.

sflow receiver owner notimeout

Use this command to configure a receiver as a non-timeout entry. Unlike entries configured with a specific timeout value, this command will be shown in show running-config and retained after reboot. As the sFlow receiver is configured as a non-timeout entry, information related to sampler and pollers will also be shown in the running-config and will be retained after reboot.

If a receiver is configured with a specific value, these configurations will not be shown in running-config. Samplers and pollers information related to this receiver will also not be shown in running-config.

Format	`sflow receiver` *`index`* `owner` *`owner-string`* `notimeout`
Mode	Global Config

Parameter	Description
index	Receiver index identifier. The range is 1 to 8.
owner-string	The owner name corresponds to the receiver name. The identity string for the receiver, the entity making use of this sFlowRcvrTable entry. The range is 127 characters. The default is a null string. The empty string indicates that the entry is currently unclaimed and the receiver configuration is reset to the default values. An entity wishing to claim an sFlowRcvrTable entry must ensure that the entry is unclaimed before trying to claim it. The entry is claimed by setting the owner string to a non-null value. The entry must be claimed before assigning a receiver to a sampler or poller.

sflow source-interface

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

Format	`sflow source-interface {`*`unit/slot/port`* `|` **`loopback`** *`loopback-id`* `|` **`tunnel`** *`tunnel-id`* `|` **`vlan`** *`vlan-id`*`}`
Mode	Global Config

Parameter	Description
unit/slot/port	VLAN or port-based routing interface.
loopback-id	Configures the loopback interface to use as the source IP address. The range of the loopback ID is 0 to 7.
tunnel-id	Configures the tunnel interface to use as the source IP address. The range of the tunnel ID is 0 to 7.
vlan-id	Configures the VLAN interface to use as the source IP address. The range of the VLAN ID is 1 to 4093.

no sflow source-interface

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

Format	`no sflow source-interface`
Mode	Global Config

show sflow receivers

Use this command to display configuration information related to the sFlow receivers.

Format	`show sflow receivers [`*`index`*`]`
Mode	Privileged EXEC

Column	Meaning
Receiver Index	The sFlow Receiver associated with the sampler/poller.
Owner String	The identity string for receiver, the entity making use of this sFlowRcvrTable entry.
Time Out	The time (in seconds) remaining before the receiver is released and stops sending samples to sFlow receiver. The no timeout value of this parameter means that the sFlow receiver is configured as a non-timeout entry.
Max Datagram Size	The maximum number of bytes that can be sent in a single sFlow datagram.
Port	The destination Layer4 UDP port for sFlow datagrams.
IP Address	The sFlow receiver IP address.
Address Type	The sFlow receiver IP address type. For an IPv4 address, the value is 1 and for an IPv6 address, the value is 2.
Datagram Version	The sFlow protocol version to be used while sending samples to sFlow receiver.

The following example shows CLI display output for this command.

```
(Extreme 220) #show sflow receivers 1
Receiver Index.............................. 1
Owner String................................ tulasi
Time out.................................... 0
IP Address:................................. 0.0.0.0
Address Type................................ 1
Port........................................ 6343
Datagram Version............................ 5
Maximum Datagram Size....................... 1400
```

The following examples show CLI display output for the command when a receiver is configured as a non-timeout entry.

```
(Extreme 220) (Routing) #show sflow receivers
Rcvr Owner                            Timeout    Max Dgram Port  IP Address
Indx String                                      Size
---- -------------------------------- ---------- --------- ----- ---------------
1    tulasi                           No Timeout 1400      6343  0.0.0.0
2                                     0          1400      6343  0.0.0.0
3                                     0          1400      6343  0.0.0.0
4                                     0          1400      6343  0.0.0.0
5                                     0          1400      6343  0.0.0.0
6                                     0          1400      6343  0.0.0.0
7                                     0          1400      6343  0.0.0.0
8                                     0          1400      6343  0.0.0.0
(Extreme 220) (Routing) #show sflow receivers 1
Receiver Index.............................. 1
Owner String................................ tulasi
Time out.................................... No Timeout
IP Address:................................. 0.0.0.0
Address Type................................ 1
Port........................................ 6343
Datagram Version............................ 5
Maximum Datagram Size....................... 1400
```

show sflow source-interface

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

Format	show sflow source-interface
Mode	Privileged EXEC

Column	Meaning
sFlow Client Source Interface	The interface ID of the physical or logical interface configured as the sFlow client source interface.
sFlow Client Source IPv4 Address	The IP address of the interface configured as the sFlow client source interface.

The following example shows CLI display output for the command.

```
(Extreme 220) (Routing) #show sflow source-interface
sFlow Client Source Interface.................. (not configured)
```

Green Ethernet Commands

This section describes the commands used to configure Green Ethernet modes on the system to save power. 200 Series software supports the following three Green Ethernet modes:

- Energy-detect mode
- Short-reach mode
- Energy-efficient Ethernet (EEE) mode

Note
Support for each Green Ethernet mode is platform dependent. The features and commands described in this section might not be available on your switch.

green-mode energy-detect

Use this command to enable energy-detect mode on an interface 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
Format	green-mode energy-detect
Mode	Interface Config

no green-mode energy-detect

Use this command to disable energy-detect mode on the interface(s).

Format	no green-mode energy-detect
Mode	Interface Config

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
Format	`green-mode eee`
Mode	Interface Config

no green-mode eee

Use this command to disable EEE mode on the interface(s).

Format	`no green-mode eee`
Mode	Interface Config

green-mode eee-lpi-history sampling-interval

Use this command to configure global EEE LPI (low-power idle) 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.

Note
The sampling interval takes effect immediately; the current and future samples are collected at this new sampling interval.

Default	3600 seconds
Format	`green-mode eee-lpi-history sampling-interval` *`30-36000`*
Mode	Global Config

no green-mode eee-lpi-history sampling-interval

Use this command to return the global EEE LPI history collection interval to the default value.

Format	`no green-mode eee-lpi-history sampling-interval`
Mode	Global Config

green-mode eee-lpi-history max-samples

Use this command to configure global EEE LPI (low-power idle) 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
Format	`green-mode eee-lpi-history max-samples` *`1-168`*
Mode	Global Config

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.

Format	`no green-mode eee-lpi-history max-samples`
Mode	Global Config

show green-mode

Use this command to display the green-mode configuration and operational status on all ports or on the specified port.

Note
The fields that display in the `show green-mode` command output depend on the Green Ethernet modes available on the hardware platform.

Format	`show green-mode [`*`unit/slot/port`*`]`
Mode	Privileged EXEC

If you do not specify a port, the command displays the following information.

Column	Meaning
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.
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 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- 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.

Column	Meaning
EEE Config	EEE Admin Mode is enabled or disabled.

The following example shows CLI display output for a system that supports all Green Ethernet features.

```
(Extreme 220) (Routing) #show green-mode
Current Power Consumption (mW)..............  11172
Power Saving (%)............................  10
Cumulative Energy Saving /Stack (W * H)...  10
Unit  Green Ethernet Features Supported
----  ------------------------------
1     Energy-Detect Short-Reach EEE LPI-History LLDP-Cap-Exchg Pwr-Usg-Est
Interface     Energy-Detect      Short-Reach-Config    Short-Reach    EEE
            Config       Opr     Auto        Forced       Opr        Config
---------  ---------  ---------  ---------  ---------  -----------   --------
1/0/1      Enabled    Active     Enabled    Disabled   Inactive      Enabled
1/0/2      Enabled    Active     Enabled    Disabled   Inactive      Enabled
1/0/3      Enabled    Active     Enabled    Disabled   Inactive      Enabled
1/0/4      Enabled    Active     Enabled    Disabled   Inactive      Enabled
1/0/5      Enabled    Active     Enabled    Disabled   Inactive      Enabled
1/0/6      Enabled    Active     Enabled    Disabled   Inactive      Enabled
1/0/7      Enabled    Active     Enabled    Disabled   Inactive      Enabled
--More-- or (q)uit
```

If you specify the port, the command displays the information in the following table.

Column	Meaning
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 in the next field.
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 is disabled. If the energy-detect operational status is active, this field displays `No energy detected`.
Short-reach auto Admin mode	Short reach auto mode is enabled or disabled.
Short-reach force Admin mode	Short reach force 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

Column	Meaning
	If the short reach operational status is active, this field displays one of the following reasons: • Short cable < 10m • Forced
EEE Admin Mode	EEE Admin Mode is enabled or disabled.
Transmit Idle Time	It is the time for which condition to move to LPI (low-power idle) 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 state. Shows the total number of Rx LPI Events since EEE counters are last cleared.
Rx Low Power Idle Duration (µSec)	This field indicates duration of Rx LPI state in 10 µs 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.
Rx Low Power Idle Duration (µSec)	This field indicates duration of Tx LPI state in 10 µs increments. Shows the total duration of Tx LPI since the EEE counters are last cleared.
Tw_sys_tx (µSec)	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 (µSec)	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 (µSec)	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 (µSec)	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 (µSec)	Integer that indicates the value of fallback Tw_sys that the local system requests from the remote system.
Remote Tw_sys_tx (µSec)	Integer that indicates the value of Tw_sys that the remote system can support.
Remote Tw_sys Echo (µSec)	Integer that indicates the value Transmit Tw_sys echoed back by the remote system.
Remote Tw_sys_rx (µSec)	Integer that indicates the value of Tw_sys that the remote system requests from the local system.
Remote Tw_sys_rx Echo (µSec)	Integer that indicates the value of Receive Tw_sys echoed back by the remote system.
Remote Fallback Tw_sys (µSec)	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.

Column	Meaning
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).

The following example shows CLI display output for on a system that supports all Green Ethernet features.

```
(Extreme 220) (Routing) #show green-mode 1/0/1
Energy Detect Admin Mode..................... Enabled
    Operational Status....................... Active
    Reason................................... No Energy Detected
Auto Short Reach Admin Mode.................. Enabled
    Forced Short Reach Admin Mode................ Enabled
    Operational Status....................... Active
    Reason................................... Forced
EEE Admin Mode............................... Enabled
    Transmit Idle Time....................... 0
    Transmit Wake Time....................... 0
    Rx Low Power Idle Event Count............ 0
    Rx Low Power Idle Duration (uSec)........ 0
    Tx Low Power Idle Event Count............ 0
    Tx Low Power Idle Duration (uSec)........ 0
    Tw_sys_tx (usec)......................... XX
    Tw_sys_tx Echo(usec)..................... XX
    Tw_sys_rx (usec)......................... XX
    Tw_sys_tx Echo(usec)..................... XX
    Fallback Tw_sys (usec)................... XX
    Remote Tw_sys_tx (usec).................. XX
    Remote Tw_sys_tx Echo(usec).............. XX
    Remote Tw_sys_rx (usec).................. XX
    Remote Tw_sys_tx Echo(usec).............. XX
    Remote fallback Tw_sys (usec)............ XX
    Tx DLL enabled........................... Yes
Tx DLL ready............................. Yes
Rx DLL enabled........................... Yes
Rx DLL ready............................. Yes
Cumulative Energy Saving (W * H).......... XX
Time Since Counters Last Cleared......... 1 day 20 hr 47 min 34 sec
```

clear green-mode statistics

Use this command to clear the following Green Ethernet mode statistics:

- EEE LPI (Low Power Idle) 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.

Note
Executing clear eee statistics clears only the EEE Transmit, Receive LPI event count, LPI duration, and Cumulative Energy Savings Estimates of the port. Other status parameters that display after executing show green-mode on page 253 retain their data.

Format	`clear green-mode statistics {`*`unit/slot/port`* `| all}`
Mode	Privileged EXEC

show green-mode eee-lpi-history

Use this command to display interface green-mode EEE LPI (low-power idle) history.

Format	`green-mode eee-lpi-history interface` *`unit/slot/port`*
Mode	Privileged EXEC

Column	Meaning
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 time spent in LPI mode by all ports in the stack, compared to the total time since the switch was last rebooted.
Sample No.	Sample index.
Sample Time	Time since last the last reboot.
%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 the last reboot.

The following example shows CLI display output for the command on a system with the EEE feature enabled.

```
(Extreme 220) (Routing) #show green-mode eee-lpi-history interface 1/0/1
Sampling Interval (sec)..................... 30
Total No. of Samples to Keep................... 168
Percentage LPI time per stack.................. 29
                                Percentage of    Percentage of
Sample     Time Since           Time spent in   Time spent in
 No.       The Sample           LPI mode since   LPI mode since
          Was Recorded          last sample      last reset
------ --------------------  --------------   --------------
10      0d:00:00:13            3                2
9       0d:00:00:44            3                2
8       0d:00:01:15            3                2
7       0d:00:01:46            3                2
6       0d:00:02:18            3                2
5       0d:00:02:49            3                2
4       0d:00:03:20            3                2
3       0d:00:03:51            3                1
```

```
2       0d:00:04:22           3               1
1       0d:00:04:53           3               1
```

Remote Monitoring Commands

Remote Monitoring (RMON) is a method of collecting a variety of data about network traffic. RMON supports 64-bit counters (RFC 3273) and High Capacity Alarm Table (RFC 3434).

Note
There is no configuration command for ether stats and high capacity ether stats. The data source for ether stats and high capacity ether stats are configured during initialization.

rmon alarm

This command sets the RMON alarm entry in the RMON alarm MIB group.

Format	`rmon alarm` *`alarm-number variable sample-interval`* `{absolute | delta} rising-threshold` *`value`* `[`*`rising-event-index`*`] falling-threshold` *`value`* `[`*`falling-event-index`*`]` **`[startup`** `{rising | falling | rising-falling}]` **`[owner`** *`string`*`]`
Mode	Global Config

Parameter	Description
`alarm-number`	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.
`variable`	The object identifier of the particular variable to be sampled. Only variables that resolve to an ASN.1 primitive type of integer.
`sample-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.
`absolute`	The value of the statistic during the last sampling period. This object is a read-only, 32-bit signed value.
`rising-threshold`*`value`*	The rising threshold for the sample statistics. The range is 2147483648 to 2147483647. The default is 1.
`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.
`falling-threshold`*`value`*	The falling threshold for the sample statistics. The range is 2147483648 to 2147483647. The default is 1.
`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.
`startup`	The alarm that may be sent. Possible values are **`rising`**, **`falling`** or **`rising-falling`** (indicating both). The default is **`rising-falling`**.
`string`	The owner string associated with the alarm entry. The default is monitorAlarm.

The following shows an example of the command.

```
(Extreme 220) (Config) # rmon alarm 1 ifInErrors.2 30 absolute rising-threshold 100 1
falling-threshold 10 2 startup rising owner myOwner
```

no rmon alarm

This command deletes the RMON alarm entry.

Format	`no rmon alarm` *`alarm-number`*
Mode	Global Config

The following shows an example of the command.

```
(Extreme 220) (Config) # no rmon alarm 1
```

rmon hcalarm

This command sets the RMON hcalarm entry in the High Capacity RMON alarm MIB group.

Format	`rmon hcalarm` *`alarm-number variable sample-interval`* `{absolute|delta}` **`rising-threshold high`** *`value`* **`low`** *`value`* **`status`** `{positive|negative}` [*`rising-event-index`*] **`falling-threshold high`** *`value`* **`low`** *`value`* **`status`** `{positive|negative}` [*`falling-event-index`*] [**`startup`** `{rising|falling|rising-falling}`] [**`owner`** *`string`*]
Mode	Global Config

Parameter	Description
`alarm-number`	An arbitrary integer index value used to uniquely identify the high capacity alarm entry. The range is 1 to 65535.
`variable`	The object identifier of the particular variable to be sampled. Only variables that resolve to an ASN.1 primitive type of integer.
`sample-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.
`absolute | delta`	The method of sampling the selected variable and calculating the value to be compared against the thresholds. Possible types are Absolute Value or Delta Value. The default is Absolute Value.
`rising-threshold high`*`value`*	The upper 32 bits of the absolute value for threshold for the sampled statistic. The range is 0 to 4294967295. The default is 0.
`rising-threshold low`*`value`*	The lower 32 bits of the absolute value for threshold for the sampled statistic. The range is 0 to 4294967295. The default is 1.
`startup`	High capacity alarm startup alarm that may be sent. Possible values are rising, falling, or rising-falling. The default is rising-falling.
`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.

Parameter	Description
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.
falling-threshold high*value*	The upper 32 bits of the absolute value for threshold for the sampled statistic. The range is 0 to 4294967295. The default is 0.
falling-threshold low*value*	The lower 32 bits of the absolute value for threshold for the sampled statistic. The range is 0 to 4294967295. The default is 1.
status	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.
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.
startup *value*	The type of alarm that is sent when the entry is enabled. Possible values are rising, falling, or rising-falling.
owner *string*	The owner string associated with the alarm entry. The default is monitorHCAlarm.

The following shows an example of the command.

```
(Extreme 220) (Config) # rmon hcalarm 1 ifInOctets.1 30 absolute rising-threshold high 1
low 100 status positive 1 falling-threshold high 1 low 10 status positive startup rising
owner myOwner
```

no rmon hcalarm

This command deletes the rmon hcalarm entry.

Format	`no rmon hcalarm` *alarm-number*
Mode	Global Config

The following shows an example of the command.

```
(Extreme 220) (Config) # no rmon hcalarm 1
```

rmon event

This command sets the RMON event entry in the RMON event MIB group.

Format	`rmon event` *event-number* [**description** *string* | **log** |**owner** *string* |**trap** *community*]
Mode	Global Config

Parameter	Description
event-number	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.
description *string*	A comment describing the event entry. The default is alarmEvent.
log	Specifies that an RMON log entry should be generated for this event.
owner*string*	Owner string associated with the entry. The default is no owner string.
trap *community*	The *SNMP* community specified by this octet string – used to send an SNMP trap. The default is no community string.

The following shows an example of the command.

```
(Extreme 220) (Config) # rmon event 1 log description test
```

no rmon event

This command deletes the rmon event entry.

Format	`no rmon event event-number`
Mode	Global Config

The following shows an example of the command.

```
(Extreme 220) (Config) # no rmon event 1
```

rmon collection history

This command sets the history control parameters of the RMON historyControl MIB group.

Note

This command is not supported on interface range. Each RMON history control collection entry can be configured on only one interface. If you try to configure on multiple interfaces, DUT displays an error.

Format	`rmon collection history index-number [buckets number| interval interval-in-sec| owner string]`
Mode	Interface Config

Parameter	Description
index-number	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.
buckets *number*	The maximum number of entries to maintain. The range is 1 to 65535. The default is 50.

Parameter	Description
interval *interval-in-sec*	The interval in seconds over which the data is sampled. The range is 1 to 3600 (one hour). The default is 1800.
owner *string*	The owner string associated with the history control entry.

The following shows an example of the command.

```
(Extreme 220) (Interface 1/0/1)# rmon collection history 1 buckets 10 interval 30 owner
myOwner
```

Note that the command is not valid for a range of interfaces, as shown in the following example.

```
(Extreme 220) (Interface 1/0/1-1/0/10)#rmon collection history 1 buckets 10 interval 30
owner myOwner
Error: 'rmon collection history' is not supported on range of interfaces.
```

no rmon collection history

This command will delete the history control group entry with the specified index number.

Format	`no rmon collection history index number`
Mode	Interface Config

The following shows an example of the command.

```
(Extreme 220) (Interface 1/0/1-1/0/10)# no rmon collection history 1
```

show rmon

This command displays the entries in the RMON alarm table.

Format	`show rmon {alarms | alarm` *alarm-index*`}`
Mode	Privileged EXEC

Column	Meaning
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.

Column	Meaning
Alarm Falling Threshold	The falling threshold for the sample statistics. The range is 2147483648 to 2147483647. The default is 1.
Alarm Falling Event Index	The index of the eventEntry that is used when a falling threshold is crossed. The range is 1 to 65535. The default is 2.
Alarm Startup Alarm	The alarm that may be sent. Possible values are rising, falling or both rising-falling. The default is rising-falling.
Alarm Owner	The owner string associated with the alarm entry. The default is monitorAlarm.

The following example shows CLI display output for the command.

```
(Extreme 220) (Routing) #show rmon alarms
Index    OID                      Owner
-----------------------------------------------
1      alarmInterval.1            MibBrowser
2      alarmInterval.1            MibBrowser
```

The following example shows CLI display output for the command.

```
(Extreme 220) (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
```

show rmon collection history

This command displays the entries in the RMON history control table.

Format	`show rmon collection history [interfaces` *`unit/slot/port`*`]`
Mode	Privileged EXEC

Column	Meaning
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.

Column	Meaning
History Control Interval	The interval in seconds over which the data is sampled. The range is 1 to 3600. The default is 1800.
History Control Owner	The owner string associated with the history control entry. The default is monitorHistoryControl.

The following example shows CLI display output for the command.

```
(Extreme 220) (Routing) #show rmon collection history
Index   Interface    Interval   Requested   Granted     Owner
                                 Samples     Samples
-------------------------------------------------------------------
1       1/0/1        30         10          10          myowner
2       1/0/1        1800       50          10          monitorHistoryControl
3       1/0/2        30         50          10          monitorHistoryControl
4       1/0/2        1800       50          10          monitorHistoryControl
5       1/0/3        30         50          10          monitorHistoryControl
6       1/0/3        1800       50          10          monitorHistoryControl
7       1/0/4        30         50          10          monitorHistoryControl
8       1/0/4        1800       50          10          monitorHistoryControl
9       1/0/5        30         50          10          monitorHistoryControl
10      1/0/5        1800       50          10          monitorHistoryControl
11      1/0/6        30         50          10          monitorHistoryControl
12      1/0/6        1800       50          10          monitorHistoryControl
13      1/0/7        30         50          10          monitorHistoryControl
14      1/0/7        1800       50          10          monitorHistoryControl
15      1/0/8        30         50          10          monitorHistoryControl
16      1/0/8        1800       50          10          monitorHistoryControl
17      1/0/9        30         50          10          monitorHistoryControl
18      1/0/9        1800       50          10          monitorHistoryControl
19      1/0/10       30         50          10          monitorHistoryControl
--More-- or (q)uit
```

The following example shows CLI display output for the command.

```
(Extreme 220) (Routing) #show rmon collection history interfaces 1/0/1
Index   Interface    Interval   Requested   Granted     Owner
                                 Samples     Samples
-------------------------------------------------------------------
1       1/0/1        30         10          10          myowner
2       1/0/1        1800       50          10          monitorHistoryControl
```

show rmon events

This command displays the entries in the RMON event table.

Format	`show rmon events`
Mode	Privileged EXEC

Parameter	Description
Event Index	An index that uniquely identifies an entry in the event table. Each such entry defines one event that is to be generated when the appropriate conditions occur. The range is 1 to 65535.
Event Description	A comment describing the event entry. The default is alarmEvent.

Parameter	Description
Event Type	The type of notification that the probe makes about the event. Possible values are None, Log, *SNMP* Trap, Log and SNMP Trap. The default is None.
Event Owner	Owner string associated with the entry. The default is monitorEvent.
Event Community	The SNMP community specific by this octet string which is used to send an SNMP trap. The default is public.
Owner	Event owner. The owner string associated with the entry.
Last time sent	The last time over which a log or a SNMP trap message is generated.

The following example shows CLI display output for the command.

```
(Extreme 220) (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
```

show rmon history

This command displays the specified entry in the RMON history table.

Format	`show rmon history` *index* {**errors** [period *seconds*] |**throughput** [period *seconds*] | **other** [period *seconds*]}
Mode	Privileged EXEC

Parameter	Description
alarm-index	An arbitrary integer index value used to uniquely identify the alarm entry. The range is 1 to 65535.
errors	Displays the error counters: CRC align errors, undersize and oversize packets, fragment packets, and jabber packets.
throughput	Displays the throughput counters: total number of octets, packets, successful broadcast and multicast packets, and port utilization.
other	Displays drop and collision counters.
period*seconds*	The period of time, in seconds, for which to display history. This parameter is accepted for the **errors**, **throughput**, and **other** options.

Column	Meaning
Maximum Table Size	Maximum number of entries that the history table can hold.
Time	Time at which the sample is collected, displayed as period seconds.
CRC Align	Number of CRC align errors.
Undersize Packets	Total number of undersize packets. Packets are less than 64 octets long (excluding framing bits, including FCS octets).
Oversize Packets	Total number of oversize packets. Packets are longer than 1518 octets (excluding framing bits, including FCS octets).

Column	Meaning
Fragments	Total number of fragment packets. Packets are not an integral number of octets in length or had a bad Frame Check Sequence (FCS), and are less than 64 octets in length (excluding framing bits, including FCS octets).
Jabbers	Total number of jabber packets. Packets are longer than 1518 octets (excluding framing bits, including FCS octets), and are not an integral number of octets in length or had a bad Frame Check Sequence (FCS).
Octets	Total number of octets received on the interface.
Packets	Total number of packets received (including error packets) on the interface.
Broadcast	Total number of good Broadcast packets received on the interface.
Multicast	Total number of good Multicast packets received on the interface.
Util	Port utilization of the interface associated with the history index specified.
Dropped Collisions	Total number of dropped collisions.

The following example shows CLI display output for the command.

```
(Extreme 220) (Routing) #show rmon history 1 errors period 300
Sample set: 1   Owner: myowner
Interface: 1/0/1   Interval: 30
Requested Samples: 10   Granted Samples: 10
Maximum table size: 1758
Time                  CRC Align  Undersize Oversize  Fragments  Jabbers
--------------------- ---------- --------- --------- ---------- -------
Jan 01 1970 21:41:43  0          0         0         0          0
Jan 01 1970 21:42:14  0          0         0         0          0
Jan 01 1970 21:42:44  0          0         0         0          0
Jan 01 1970 21:43:14  0          0         0         0          0
Jan 01 1970 21:43:44  0          0         0         0          0
Jan 01 1970 21:44:14  0          0         0         0          0
Jan 01 1970 21:44:45  0          0         0         0          0
Jan 01 1970 21:45:15  0          0         0         0          0
Jan 01 1970 21:45:45  0          0         0         0          0
Jan 01 1970 21:46:15  0          0         0         0          0
```

The following example shows CLI display output for the command.

```
(Extreme 220) (Routing) #show rmon history 1 throughput period 300
Sample set: 1   Owner: myowner
Interface: 1/0/1   Interval: 30
Requested Samples: 10   Granted Samples: 10
Maximum table size: 1758
Time                  Octets     Packets   Broadcast Multicast  Util
--------------------- ---------- --------- --------- ---------- --------
Jan 01 1970 21:41:43 0          0         0         0          1
Jan 01 1970 21:42:14 0          0         0         0          1
Jan 01 1970 21:42:44 0          0         0         0          1
Jan 01 1970 21:43:14 0          0         0         0          1
Jan 01 1970 21:43:44 0          0         0         0          1
Jan 01 1970 21:44:14 0          0         0         0          1
Jan 01 1970 21:44:45 0          0         0         0          1
Jan 01 1970 21:45:15 0          0         0         0          1
Jan 01 1970 21:45:45 0          0         0         0          1
Jan 01 1970 21:46:15 0          0         0         0          1
(Extreme 220) (Routing) #show rmon history 1 other period 300
Sample set: 1   Owner: myowner
Interface: 1/0/1   Interval: 30
Requested Samples: 10   Granted Samples: 10
```

```
Maximum table size: 1758
Time                 Dropped Collisions
-------------------- ------- ----------
Jan 01 1970 21:41:43 0       0
Jan 01 1970 21:42:14 0       0
Jan 01 1970 21:42:44 0       0
Jan 01 1970 21:43:14 0       0
Jan 01 1970 21:43:44 0       0
Jan 01 1970 21:44:14 0       0
Jan 01 1970 21:44:45 0       0
Jan 01 1970 21:45:15 0       0
Jan 01 1970 21:45:45 0       0
Jan 01 1970 21:46:15 0       0
```

show rmon log

This command displays the entries in the RMON log table.

Format	`show rmon log [event-index]`
Mode	Privileged EXEC

Column	Meaning
Maximum table size	Maximum number of entries that the log table can hold.
Event	Event index for which the log is generated.
Description	A comment describing the event entry for which the log is generated.
Time	Time at which the event is generated.

The following example shows CLI display output for the command.

```
(Extreme 220) (Routing) #show rmon log
Event   Description                  Time
-----------------------------------------------
```

The following example shows CLI display output for the command.

```
(Extreme 220) (Routing) #show rmon log 1
Maximum table size: 10
Event   Description                  Time
-----------------------------------------------
```

show rmon statistics interfaces

This command displays the RMON statistics for the given interfaces.

Format	`show rmon statistics interfaces unit/slot/port`
Mode	Privileged EXEC

Column	Meaning
Port	unit/slot/port
Dropped	Total number of dropped events on the interface.

Column	Meaning
Octets	Total number of octets received on the interface.
Packets	Total number of packets received (including error packets) on the interface.
Broadcast	Total number of good broadcast packets received on the interface.
Multicast	Total number of good multicast packets received on the interface.
CRC Align Errors	Total number of packets received have a length (excluding framing bits, including FCS octets) of between 64 and 1518 octets inclusive.
Collisions	Total number of collisions on the interface.
Undersize Pkts	Total number of undersize packets. Packets are less than 64 octets long (excluding framing bits, including FCS octets).
Oversize Pkts	Total number of oversize packets. Packets are longer than 1518 octets (excluding framing bits, including FCS octets).
Fragments	Total number of fragment packets. Packets are not an integral number of octets in length or had a bad Frame Check Sequence (FCS), and are less than 64 octets in length (excluding framing bits, including FCS octets).
Jabbers	Total number of jabber packets. Packets are longer than 1518 octets (excluding framing bits, including FCS octets), and are not an integral number of octets in length or had a bad FCS.
64 Octets	Total number of packets which are 64 octets in length (excluding framing bits, including FCS octets).
65-127 Octets	Total number of packets which are between 65 and 127 octets in length (excluding framing bits, including FCS octets).
128-255 Octets	Total number of packets which are between 128 and 255 octets in length (excluding framing bits, including FCS octets).
256-511 Octets	Total number of packets which are between 256 and 511 octets in length (excluding framing bits, including FCS octets).
512-1023 Octets	Total number of packets which are between 512 and 1023 octets in length (excluding framing bits, including FCS octets).
1024-1518 Octets	Total number of packets which are between 1024 and 1518 octets in length (excluding framing bits, including FCS octets).
HC Overflow Pkts	Total number of HC overflow packets.
HC Overflow Octets	Total number of HC overflow octets.
HC Overflow Pkts 64 Octets	Total number of HC overflow packets which are 64 octets in length
HC Overflow Pkts 65 - 127 Octets	Total number of HC overflow packets which are between 65 and 127 octets in length.
HC Overflow Pkts 128 - 255 Octets	Total number of HC overflow packets which are between 128 and 255 octets in length.
HC Overflow Pkts 256 - 511 Octets	Total number of HC overflow packets which are between 256 and 511 octets in length.
HC Overflow Pkts 512 - 1023 Octets	Total number of HC overflow packets which are between 512 and 1023 octets in length.
HC Overflow Pkts 1024 - 1518 Octets	Total number of HC overflow packets which are between 1024 and 1518 octets in length.

The following example shows CLI display output for the command.

```
(Extreme 220) (Routing) # show rmon statistics interfaces 1/0/1
Port: 1/0/1
Dropped: 0
Octets: 0  Packets: 0
Broadcast: 0  Multicast: 0
CRC Align Errors: 0  Collisions: 0
Undersize Pkts: 0  Oversize Pkts: 0
Fragments: 0  Jabbers: 0
64 Octets: 0  65 - 127 Octets: 0
128 - 255 Octets: 0  256 - 511 Octets: 0
512 - 1023 Octets: 0  1024 - 1518 Octets: 0
HC Overflow Pkts: 0  HC Pkts: 0
HC Overflow Octets: 0  HC Octets: 0
HC Overflow Pkts 64 Octets: 0  HC Pkts 64 Octets: 0
HC Overflow Pkts 65 - 127 Octets: 0  HC Pkts 65 - 127 Octets: 0
HC Overflow Pkts 128 - 255 Octets: 0  HC Pkts 128 - 255 Octets: 0
HC Overflow Pkts 256 - 511 Octets: 0  HC Pkts 256 - 511 Octets: 0
HC Overflow Pkts 512 - 1023 Octets: 0  HC Pkts 512 - 1023 Octets: 0
HC Overflow Pkts 1024 - 1518 Octets: 0  HC Pkts 1024 - 1518 Octets: 0
```

show rmon hcalarms

This command displays the entries in the RMON high-capacity alarm table.

Format	`show rmon {hcalarms|hcalarm` *`alarm-index`*`}`
Mode	Privileged EXEC

Parameter	Description
`alarm-index`	An arbitrary integer index value used to uniquely identify the high capacity alarm entry. The range is 1 to 65535.

For a description of the parameters in the command output, refer to the command rmon hcalarm on page 259.

The following example shows CLI display output for the command.

```
(Extreme 220) (Routing) #show rmon hcalarms
Index    OID                      Owner
-----------------------------------------------
1      alarmInterval.1            MibBrowser
2      alarmInterval.1            MibBrowser
(Extreme 220) (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
```

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 OCT 2017 (START) and 21:00 12 OCT 2017 (END) or schedule it on every Monday, Wednesday, and Friday from 9:00 (START) to 21:00 (END).

You can receive the statistics in the following ways:

- User requests through the CLI for a set of counters.
- Configuring the device to display statistics using syslog or email alert. The syslog or email alert messages are sent by the statistics application at END time.

You can configure the device to display statistics on the console. The collected statistics are presented on the console at END time.

stats group

This command creates a new group with the specified id or name and configures the time range and the reporting mechanism for that group.

Format	`stats group` *`group id`* `timerange` *`time-range-name`* `reporting` *`reporting-methods`*
Mode	Global Config

Parameter	Description
group id	ID or name of the group of statistics to apply on the interface. You can enter either the word or the corresponding numeral. Valid values are: • 1: received • 2: received-errors • 3: transmitted • 4: transmitted-errors • 5: received-transmitted • 6: port-utilization • 7: congestion There is no default value.
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.
reporting-methods	Report the statistics to the configured method. Valid values are: • none • console • syslog • email The default is none.

The following examples show how the command could be entered.

```
(Extreme 220) (Config) # stats group received timerange test reporting console email syslog
(Extreme 220) (Config) # stats group received-errors timerange test reporting email syslog
(Extreme 220) (Config) # stats group received-transmitted timerange test reporting none
```

no stats group

This command deletes the configured group.

Format	`no stats group` *`group id|name`*
Mode	Global Config

The following example shows how the command could be entered.

```
(Extreme 220) (Config) # no stats group received
(Extreme 220) (Config) # no stats group received-errors
(Extreme 220) (Config) # no stats group received-transmitted
```

stats flow-based

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.

Format	`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`*`}]`
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`*	The source IP address.
`dstip` *`ip-address`*	The destination IP address.
`srcmac` *`mac-address`*	The source MAC address.
`dstmac` *`mac-address`*	The destination MAC address.
`srctcpport` *`portid`*	The source TCP port number.
`dsttcpport` *`portid`*	The destination TCP port number.
`srcudpport` *`portid`*	The source UDP port number.
`dstudpport` *`portid`*	The destination UDP port number.

The following example shows how the command could be entered.

```
(Extreme 220) (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
(Extreme 220) (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
```

no stats flow-based

This command deletes flow-based statistics.

Format	`no stats flow-based` *`rule-id`*
Mode	Global Config

The following example shows how the command could be entered.

```
(Extreme 220) (Config) # no stats flow-based 1
(Extreme 220) (Config) # no stats flow-based 2
```

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.

Format	stats flow-based reporting *list of reporting methods*
Mode	Global Config

The following example shows how the command could be entered.

```
(Extreme 220) (Config) # stats flow-based reporting console email syslog
(Extreme 220) (Config) # stats flow-based reporting email syslog
(Extreme 220) (Config) # stats flow-based reporting none
```

stats group

This command applies the group specified on an interface or interface-range.

Format	stats group *group id* | *name*
Mode	Interface Config

Parameter	Description
group id	The unique identifier for the group.
name	The name of the group.

The following example shows how the command could be entered.

```
(Extreme 220) (Interface 1/0/1-1/0/10)# stats group 1
(Extreme 220) (Interface 1/0/1-1/0/10)# stats group 2
```

no stats group

This command deletes the interface or interface-range from the group specified.

Format	no stats group *group id* | *name*
Mode	Interface Config

The following example shows how the command could be entered.

```
(Extreme 220) (Interface 1/0/1-1/0/10)# no stats group 1
(Extreme 220) (Interface 1/0/1-1/0/10)# no stats group 2
```

stats flow-based

This command applies the flow-based rule specified by the ID on an interface or interface-range.

Format	stats flow-based *rule-id*
Mode	Interface Config

Parameter	Description
rule-id	The unique identifier for the flow-based rule.

The following example shows how the command could be entered.

```
(Extreme 220) (Interface 1/0/1-1/0/10)# stats flow-based 1
(Extreme 220) (Interface 1/0/1-1/0/10)# stats flow-based 2
```

no stats flow-based

This command deletes the interface or interface-range from the flow-based rule specified.

Format	`no stats flow-based` *`rule-id`*
Mode	Interface Config

The following example shows how the command could be entered.

```
(Extreme 220) (Config) (Interface 1/0/1-1/0/10)# no stats flow-based 1
(Extreme 220) (Config) (Interface 1/0/1-1/0/10)# no stats flow-based 2
```

show stats group

This command displays the configured time range 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.

Format	`show stats group` *`group id	name`*
Mode	Privileged EXEC

Parameter	Description
`group id`	The unique identifier for the group.
`name`	The name of the group.

The following example shows CLI display output for the command.

```
(Extreme 220) (Routing) #show stats group received
Group: received
Time Range: test
Interface List
-----------------
1/0/2, 1/0/4, lag 1
Counter ID                 Interface  Counter Value
-------------------------  ---------  -------------
Rx Total                     1/0/2      951600
Rx Total                     1/0/4      304512
Rx Total                     lag 1      0
Rx 64                        1/0/2      0
Rx 64                        1/0/4      4758
Rx 64                        lag 1      0
Rx 65to128                   1/0/2      0
Rx 65to128                   1/0/4      0
Rx 65to128                   lag 1      0
Rx 128to255                  1/0/2      4758
Rx 128to255                  1/0/4      0
Rx 128to255                  lag 1      0
Rx 256to511                  1/0/2      0
```

The following example shows CLI display output for the command.

```
(Extreme 220) (Routing) #show stats group port-utilization
Group: port-utilization
Time Range: test
Interface List
--------------
1/0/2, 1/0/4, lag 1
Interface  Utilization (%)
---------  ---------------
1/0/2      0
1/0/4      0
lag 1      0
```

show stats flow-based

This command displays the configured time range, flow-based rule parameters, and the interface list for the flow specified.

Format	`show stats flow-based` *`rule-id`* `| all`
Mode	Privileged EXEC

Parameter	Description
`rule-id`	The unique identifier for the flow-based rule.

The following example shows CLI display output for the command.

```
(Extreme 220) (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
--------------
1/0/1 - 1/0/2
Interface  Hit Count
---------  ---------
1/0/1      100
1/0/2      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
--------------
1/0/1 - 1/0/2
Interface  Hit Count
---------  ---------
```

```
1/0/1      100
1/0/2      0
```

The following example shows CLI display output for the command.

```
(Extreme 220) (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
--------------
1/0/1 - 1/0/2
Interface  Hit Count
---------  ---------
1/0/1      100
1/0/2      0
```

5 Switching Commands

This chapter describes the switching commands available in the 200 Series CLI.

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

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

Port Configuration Commands

This section describes the commands used to view and configure port settings.

interface

This command gives you access to the Interface Config mode, which allows you to enable or modify the operation of an interface (port). You can also specify a range of ports to configure at the same time by specifying the starting unit/slot/port and ending unit/slot/port, separated by a hyphen.

Format	`interface {`*`unit/slot/port	unit/slot/port(startrange)-unit/slot/port(endrange)`*`}`
Mode	Global Config

The following example enters Interface Config mode for port 1/0/1:

```
(Extreme 220) #configure
(Extreme 220) (Config) #interface 1/0/1
(Extreme 220) (interface 1/0/1)#
```

The following example enters Interface Config mode for ports 1/0/1 through 1/0/4:

```
(Extreme 220) #configure
(Extreme 220) (Config) #interface 1/0/1-1/0/4
(Extreme 220) (interface 1/0/1-1/0/4)#
```

auto-negotiate all

This command enables automatic negotiation on all ports.

Default	Enabled
Format	`auto-negotiate all`
Mode	Global Config

no auto-negotiate all

This command disables automatic negotiation on all ports.

Format	`no auto-negotiate all`
Mode	Global Config

description

Use this command to create an alpha-numeric description of an interface or range of interfaces.

Format	`description` *`description`*
Mode	Interface Config

media-type

Use this command to change between fiber and copper mode on the combo port.

- Combo Port: A port or an interface that can operate in either copper or in fiber mode.
- Copper and Fiber port: A port that uses copper a medium for communication (for example, RJ45 ports). A fiber port uses the fiber optics as a medium for communication (for example, example SFP ports).

Default	Auto-select, SFP preferred
Format	`media-type {auto-select | rj45 | sfp }`
Mode	Interface Config

The following modes are supported by the `media-type` command.

- Auto-select, SFP preferred: The medium is selected automatically based on the physical medium presence. However, when both the fiber and copper links are connected, the fiber link takes precedence and the fiber link is up.
- Auto-select, RJ45 preferred: The medium is selected automatically based on the physical medium presence. However, when both the fiber and copper links are connected, the copper link takes precedence and the copper link is up.
- SFP: Only the fiber medium works. The copper medium is always down.
- RJ45: Only the copper medium works. The fiber medium is always down.

no media-type

Use this command to revert the media-type configuration and configure the default value on the interface.

Format	`no media-type`
Mode	Interface Config

mtu

Use this 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 (Link Aggregation Group)* interfaces. For the standard 200 Series implementation, the MTU size is an integer between 1500 and 9198 for both tagged packets and untagged packets.

Note
To receive and process packets, the Ethernet MTU must include any extra bytes that layer-2 headers might require. To configure the IP MTU size, which is the maximum size of the IP packet (IP Header + IP payload), see ip mtu on page 512.

Default	1500 (untagged)
Format	`mtu 1500-9198`
Mode	Interface Config

no mtu

This command sets the default MTU size (in bytes) for the interface.

Format	`no mtu`
Mode	Interface Config

shutdown

This command disables a port or range of ports.

Note
You can use the shutdown command on physical and port-channel (*LAG*) interfaces, but not on VLAN routing interfaces.

Default	Enabled
Format	`shutdown`
Mode	Interface Config

no shutdown

This command enables a port.

Format	`no shutdown`
Mode	Interface Config

shutdown all

This command disables all ports.

Note
You can use the shutdown all command on physical and port-channel (*LAG*) interfaces, but not on VLAN routing interfaces.

Default	Enabled
Format	`shutdown all`
Mode	Global Config

no shutdown all

This command enables all ports.

Format	`no shutdown all`
Mode	Global Config

speed

Use this command to enable or disable auto-negotiation and set the speed that will be advertised by that port. The duplex parameter allows you to set the advertised speed for both half as well as full duplex mode.

Use the auto keyword to enable auto-negotiation on the port. Use the command without the auto keyword to ensure auto-negotiation is disabled and to set the port speed and mode according to the command values. If auto-negotiation is disabled, the speed and duplex mode must be set.

Default	Auto-negotiation is enabled.
Format	`speed auto {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]` `speed {10|100|1000|2.5G|10G|20G|25G|40G|50G|100G} {half-duplex|full-duplex}.`
Mode	Interface Config

speed all

This command sets the speed and duplex setting for all interfaces if auto-negotiation is disabled. If auto-negotiation is enabled, an error message is returned. Use the `no auto-negotiate` command to disable.'

Default	Auto-negotiation is enabled. Adv. is 10h, 10f, 100h, 100f, 1000f.
Format	`speed all {100 | 10} {half-duplex | full-duplex}`
Mode	Global Config

show interface media-type

Use this command to display the media-type configuration of the interface.

Format	`show interface media-type`
Mode	Privileged EXEC

The following information is displayed for the command.

Column	Meaning
Port	Interface in unit/slot/port format.
Configured Media Type	The media type for the interface. • auto-select: The media type is automatically selected. The preferred media type is displayed. • RJ45 • SFP
Active	Displays the current operational state of the combo port.

The following command shows the command output:

```
(Extreme 220) (Routing) #show interface media-type
Port       Configured Media Type         Active
---------  ----------------------------  ------
0/21       SFP                           RJ45
0/22       auto-select, SFP preferred    Down
0/23       auto-select, SFP preferred    RJ45
0/24       auto-select, SFP preferred    Down
```

show port

This command displays port information.

Format	`show port {`*`intf-range`*` | all}`
Mode	Privileged EXEC

Column	Meaning
Interface	unit/slot/port
Type	If not blank, this field indicates that this port is a special type of port. The possible values are: • Mirror — this port is a monitoring port. For more information, see Port Mirroring Commands on page 402. • PC Mbr— this port is a member of a port-channel (*LAG*). • Probe — this port is a probe port.

Column	Meaning
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 to send a trap when link status changes. The factory default is enabled.
LACP Mode	LACP is enabled or disabled on this port.

The following command shows an example of the command output for all ports.

```
(Extreme 220) (Routing) #show port all
                 Admin     Physical   Physical   Link   Link    LACP   Actor
Intf      Type   Mode      Mode       Status     Status Trap    Mode   Timeout
--------- ------ --------- ---------- ---------- ------ ------- ------ --------
0/1              Enable    Auto       100 Full   Up     Enable  Enable long
0/2              Enable    Auto       100 Full   Up     Enable  Enable long
0/3              Enable    Auto                  Down   Enable  Enable long
0/4              Enable    Auto       100 Full   Up     Enable  Enable long
0/5              Enable    Auto       100 Full   Up     Enable  Enable long
0/6              Enable    Auto       100 Full   Up     Enable  Enable long
0/7              Enable    Auto       100 Full   Up     Enable  Enable long
0/8              Enable    Auto       100 Full   Up     Enable  Enable long
1/1              Enable                          Down   Disable N/A    N/A
1/2              Enable                          Down   Disable N/A    N/A
1/3              Enable                          Down   Disable N/A    N/A
1/4              Enable                          Down   Disable N/A    N/A
1/5              Enable                          Down   Disable N/A    N/A
1/6              Enable                          Down   Disable N/A    N/A
```

The following command shows an example of the command output for a range of ports.

```
(Extreme 220) (Routing) #show port 0/1-1/6
                 Admin     Physical   Physical   Link   Link    LACP   Actor
Intf      Type   Mode      Mode       Status     Status Trap    Mode   Timeout
--------- ------ --------- ---------- ---------- ------ ------- ------ --------
0/1              Enable    Auto       100 Full   Up     Enable  Enable long
0/2              Enable    Auto       100 Full   Up     Enable  Enable long
0/3              Enable    Auto                  Down   Enable  Enable long
0/4              Enable    Auto       100 Full   Up     Enable  Enable long
0/5              Enable    Auto       100 Full   Up     Enable  Enable long
0/6              Enable    Auto       100 Full   Up     Enable  Enable long
0/7              Enable    Auto       100 Full   Up     Enable  Enable long
0/8              Enable    Auto       100 Full   Up     Enable  Enable long
1/1              Enable                          Down   Disable N/A    N/A
1/2              Enable                          Down   Disable N/A    N/A
1/3              Enable                          Down   Disable N/A    N/A
1/4              Enable                          Down   Disable N/A    N/A
1/5              Enable                          Down   Disable N/A    N/A
1/6              Enable                          Down   Disable N/A    N/A
```

show port advertise

Use this command to display the local administrative link advertisement configuration, local operational link advertisement, and the link partner advertisement for an interface. It also displays priority Resolution for speed and duplex as per 802.3 Annex 28B.3. It displays the Auto negotiation state, PHY Master/Slave Clock configuration, and Link state of the port.

If the link is down, the Clock is displayed as No Link, and a dash is displayed against the Oper Peer advertisement, and Priority Resolution. If Auto negotiation is disabled, then the admin Local Link advertisement, operational local link advertisement, operational peer advertisement, and Priority resolution fields are not displayed.

If this command is executed without the optional unit/slot/port parameter, then it displays the Auto-negotiation state and operational Local link advertisement for all the ports. Operational link advertisement will display speed only if it is supported by both local as well as link partner. If auto-negotiation is disabled, then operational local link advertisement is not displayed.

Format	`show port advertise [unit/slot/port]`
Mode	Privileged EXEC

The following commands show the command output with and without the optional parameter:

```
(Extreme 220) (Switching)#show port advertise 0/1
Port: 0/1
Type: Gigabit - Level
Link State: Down
Auto Negotiation: Enabled
Clock: Auto
                              1000f 1000h 100f 100h 10f 10h
                              ----- ----- ---- ---- --- ---
Admin Local Link Advertisement no    no    yes  no   yes no
Oper Local Link Advertisement  no    no    yes  no   yes no
Oper Peer Advertisement            no        no        yes      yes      yes yes
Priority Resolution            -     -     yes  -    -   -
(Extreme 220) (Switching)#show port advertise
Port      Type                                Neg      Operational Link Advertisement
--------- ------------------------------ ----------- ------------------------------
0/1   Gigabit - Level                     Enabled  1000f, 100f, 100h, 10f, 10h
0/2   Gigabit - Level                     Enabled  1000f, 100f, 100h, 10f, 10h
0/3   Gigabit - Level                     Enabled  1000f, 100f, 100h, 10f, 10h
```

show port description

This command displays the interface description. Instead of 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.

Format	`show port description unit/slot/port`
Mode	Privileged EXEC

Column	Meaning
Interface	unit/slot/port
ifIndex	The interface index number associated with the port.

Column	Meaning
Description	The alpha-numeric description of the interface created by the `description`command (see description on page 279).
MAC address	The MAC address of the port. The format is 6 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB.
Bit Offset Val	The bit offset value.

The following example shows CLI display output for the command.

```
(Extreme 220) (Switching) #show port description 0/1
Interface...........0/1
ifIndex.............1
Description.........
MAC address.........00:10:18:82:0C:10
Bit Offset Val......1
```

Spanning Tree Protocol Commands

This section describes the commands used to configure *STP (Spanning Tree Protocol)*. STP helps prevent network loops, duplicate messages, and network instability.

Note
STP is enabled on the switch and on all ports and LAGs by default.

Note
If STP is disabled, the system does not forward BPDU messages.

spanning-tree

This command sets the spanning-tree operational mode to enabled.

Default	Enabled
Format	`spanning-tree`
Mode	Global Config

no spanning-tree

This command sets the spanning-tree operational mode to disabled. While disabled, the spanning-tree configuration is retained and can be changed, but is not activated.

Format	`no spanning-tree`
Mode	Global Config

spanning-tree auto-edge

Use this command to allow the interface to become an edge port if it does not receive any BPDUs within a given amount of time.

Default	Enabled
Format	`spanning-tree auto-edge`
Mode	Interface Config

no spanning-tree auto-edge

This command resets the auto-edge status of the port to the default value.

Format	`no spanning-tree auto-edge`
Mode	Interface Config

spanning-tree backbonefast

Use this command to enable the detection of indirect link failures and accelerate spanning tree convergence on PVSTP configured switches.

Backbonefast accelerates finding an alternate path when an indirect link to the root port goes down.

Backbonefast can be configured even if the switch is configured for MST(RSTP) or PVST mode. It only has an effect when the switch is configured for the PVST mode.

If a backbonefast-enabled switch receives an inferior BPDU from its designated switch on a root or blocked port, it sets the maximum aging time on the interfaces on which it received the inferior BPDU if there are alternate paths to the designated switch. This allows a blocked port to immediately move to the listening state where the port can be transitioned to the forwarding state in the normal manner.

On receipt of an inferior BPDU from a designated bridge, backbonefast enabled switches send a Root Link Query (RLQ) request to all non-designated ports except the port from which it received the inferior BPDU. This check validates that the switch can receive packets from the root on ports where it expects to receive BPDUs. The port from which the original inferior BPDU was received is excluded because it has already encountered a failure. Designated ports are excluded as they do not lead to the root.

On receipt of an RLQ response, if the answer is negative, the receiving port has lost connection to the root and its BPDU is immediately aged out. If all nondesignated ports have already received a negative answer, the whole bridge has lost the root and can start the *STP* calculation from scratch.

If the answer confirms the switch can access the root bridge on a port, it can immediately age out the port on which it initially received the inferior BPDU.

A bridge that sends an RLQ puts its bridge ID in the PDU. This ensures that it does not flood the response on designated ports.

A bridge that receives an RLQ and has connectivity to the root forwards the query toward the root through its root port.

A bridge that receives a RLQ request and does not have connectivity to the root (switch bridge ID is different from the root bridge ID in the query) or is the root bridge immediately answers the query with its root bridge ID.

RLQ responses are flooded on designated ports.

Default	NA
Format	`spanning-tree backbonefast`
Mode	Global Config

no spanning-tree backbonefast

This command disables backbonefast.

Note
PVRSTP embeds support for FastBackbone and FastUplink. Even if FastUplink and FastBackbone are configured, they are effective only in PVSTP mode.

Format	`no spanning-tree backbonefast`
Mode	Global Config

spanning-tree bpdufilter

Use this command to enable BPDU Filter on an interface or range of interfaces.

Default	Disabled
Format	`spanning-tree bpdufilter`
Mode	Interface Config

no spanning-tree bpdufilter

Use this command to disable BPDU Filter on the interface or range of interfaces.

Default	Disabled
Format	`no spanning-tree bpdufilter`
Mode	Interface Config

spanning-tree bpdufilter default

Use this command to enable BPDU Filter on all the edge port interfaces.

Default	Disabled
Format	`spanning-tree bpdufilter default`
Mode	Global Config

no spanning-tree bpdufilter default

Use this command to disable BPDU Filter on all the edge port interfaces.

Default	Disabled
Format	`no spanning-tree bpdufilter default`
Mode	Global Config

spanning-tree bpduflood

Use this command to enable BPDU Flood on an interface or range of interfaces.

Default	Disabled
Format	`spanning-tree bpduflood`
Mode	Interface Config

no spanning-tree bpduflood

Use this command to disable BPDU Flood on the interface or range of interfaces.

Default	Disabled
Format	`no spanning-tree bpduflood`
Mode	Interface Config

spanning-tree bpduguard

Use this command to enable BPDU Guard on the switch.

Default	Disabled
Format	`spanning-tree bpduguard`
Mode	Global Config

no spanning-tree bpduguard

Use this command to disable BPDU Guard on the switch.

Default	Disabled
Format	`no spanning-tree bpduguard`
Mode	Global Config

spanning-tree bpdumigrationcheck

Use this command to force a transmission of rapid spanning tree (RSTP) and *MSTP (Multiple Spanning Tree Protocol)* BPDUs. Use the unit/slot/port parameter to transmit a BPDU from a specified interface, or use the all keyword to transmit RST or MST BPDUs from all interfaces. This command forces the BPDU transmission when you execute it, so the command does not change the system configuration or have a no version.

Format	`spanning-tree bpdumigrationcheck {`*`unit/slot/port`*` | all}`
Mode	Global Config

spanning-tree configuration name

This command sets the Configuration Identifier Name for use in identifying the configuration that this switch is currently using. The name is a string of up to 32 characters.

Default	base MAC address in hexadecimal notation
Format	`spanning-tree configuration name` *`name`*
Mode	Global Config

no spanning-tree configuration name

This command resets the Configuration Identifier Name to its default.

Format	`no spanning-tree configuration name`
Mode	Global Config

spanning-tree configuration revision

This command sets the Configuration Identifier Revision Level for use in identifying the configuration that this switch is currently using. The Configuration Identifier Revision Level is a number in the range of 0 to 65535.

Default	0
Format	`spanning-tree configuration revision` *`0–65535`*
Mode	Global Config

no spanning-tree configuration revision

This command sets the Configuration Identifier Revision Level for use in identifying the configuration that this switch is currently using to the default value.

Format	`no spanning-tree configuration revision`
Mode	Global Config

spanning-tree cost

Use this command to configure the external path cost for port used by a MST instance. When the **`auto`** keyword is used, the path cost from the port to the root bridge is automatically determined by the speed of the interface. To configure the cost manually, specify a cost value from 1–200000000.

Default	auto
Format	`spanning-tree cost {cost | auto}`
Mode	Interface Config

no spanning-tree cost

This command resets the auto-edge status of the port to the default value.

Format	`no spanning-tree cost`
Mode	Interface Config

spanning-tree edgeport

This command specifies that an interface (or range of interfaces) is an Edge Port within the common and internal spanning tree. This allows this port to transition to Forwarding State without delay.

Format	`spanning-tree edgeport`
Mode	Interface Config

no spanning-tree edgeport

This command specifies that this port is not an Edge Port within the common and internal spanning tree.

Format	`no spanning-tree edgeport`
Mode	Interface Config

spanning-tree forward-time

This command sets the Bridge Forward Delay parameter to a new value for the common and internal spanning tree. The forward-time value is in seconds within a range of 4 to 30, with the value being greater than or equal to "(Bridge Max Age / 2) + 1".

Default	15
Format	`spanning-tree forward-time` *`4-30`*
Mode	Global Config

no spanning-tree forward-time

This command sets the Bridge Forward Delay parameter for the common and internal spanning tree to the default value.

Format	`no spanning-tree forward-time`
Mode	Global Config

spanning-tree guard

This command selects whether loop guard or root guard is enabled on an interface or range of interfaces. If neither is enabled, then the port operates in accordance with the multiple spanning tree protocol.

Default	none
Format	`spanning-tree guard {none | root | loop}`
Mode	Interface Config

no spanning-tree guard

This command disables loop guard or root guard on the interface.

Format	`no spanning-tree guard`
Mode	Interface Config

spanning-tree max-age

This command sets the Bridge Max Age parameter to a new value for the common and internal spanning tree. The max-age value is in seconds within a range of 6 to 40, with the value being less than or equal to 2 x (Bridge Forward Delay - 1).

Default	20
Format	`spanning-tree max-age` *`6-40`*
Mode	Global Config

no spanning-tree max-age

This command sets the Bridge Max Age parameter for the common and internal spanning tree to the default value.

Format	`no spanning-tree max-age`
Mode	Global Config

spanning-tree max-hops

This command sets the Bridge Max Hops parameter to a new value for the common and internal spanning tree. The max-hops value is a range from 6 to 40.

Default	20
Format	`spanning-tree max-hops` *`6-40`*
Mode	Global Config

no spanning-tree max-hops

This command sets the Bridge Max Hops parameter for the common and internal spanning tree to the default value.

Format	`no spanning-tree max-hops`
Mode	Global Config

spanning-tree mode

This command configures global spanning tree mode per VLAN spanning tree, Rapid-PVST, MST, RSTP or *STP*. Only one of *MSTP* (RSTP), PVST or RPVST can be enabled on a switch.

When PVSTP or rapid PVSTP (PVRSTP) is enabled, MSTP/RSTP/STP is operationally disabled. To reenable MSTP/RSTP/STP, disable PVSTP/PVRSTP. By default, 200 Series has MSTP enabled. In PVSTP or PVRSTP mode, BPDUs contain per-VLAN information instead of the common spanning-tree information (MST/RSTP).

PVSTP maintains independent spanning tree information about each configured VLAN. PVSTP uses IEEE 802.1Q trunking and allows a trunked VLAN to maintain blocked or forwarding state per port on a per-VLAN basis. This allows a trunk port to be forwarded on some VLANs and blocked on other VLANs.

PVRSTP is based on the IEEE 8012.1w standard. It supports fast convergence IEEE 802.1D. PVRSTP is compatible with IEEE 802.1D spanning tree. PVRSTP sends BPDUs on all ports, instead of only the root bridge sending BPDUs, and supports the discarding, learning, and forwarding states.

When the mode is changed to PVRSTP, version 0 STP BPDUs are no longer transmitted and version 2 PVRSTP BPDUs that carry per-VLAN information are transmitted on the VLANs enabled for spanning-tree. If a version 0 BPDU is seen, PVRSTP reverts to sending version 0 BPDUs.

Per VLAN Rapid Spanning Tree Protocol (PVRSTP) embeds support for PVSTP FastBackbone and FastUplink. There is no provision to enable or disable these features in PVRSTP.

Default	Disabled
Format	`spanning-tree mode {mst | pvst | rapid-pvst | stp | rstp }`
Mode	Global Config

no spanning-tree mode

This command globally configures the switch to the default 200 Series spanning-tree mode, *MSTP*.

Format	`no spanning-tree mode { pvst | rapid-pvst }`
Mode	Global Configuration

spanning-tree mst

This command sets the Path Cost or Port Priority for this port within the multiple spanning tree instance or in the common and internal spanning tree. If you specify an mstid parameter that corresponds to an existing multiple spanning tree instance, the configurations are done for that multiple spanning tree instance. If you specify 0 (defined as the default CIST ID) as the mstid, the configurations are done for the common and internal spanning tree instance.

If you specify the **`cost`** option, the command sets the path cost for this port within a multiple spanning tree instance or the common and internal spanning tree instance, depending on the mstid parameter. You can set the path cost as a number in the range of 1 to 200000000 or auto. If you select auto the path cost value is set based on Link Speed.

If you specify the **`port-priority`** option, this command sets the priority for this port within a specific multiple spanning tree instance or the common and internal spanning tree instance, depending on the mstid parameter. The port-priority value is a number in the range of 0 to 240 in increments of 16.

Default	• cost—auto • port-priority—128
Format	`spanning-tree mst` *`mstid`* `{{cost` *`1-200000000`* `| auto} | port-priority` *`0-240`*`}`
Mode	Interface Config

no spanning-tree mst

This command sets the Path Cost or Port Priority for this port within the multiple spanning tree instance, or in the common and internal spanning tree to the respective default values. If you specify an mstid parameter that corresponds to an existing multiple spanning tree instance, you are configuring that multiple spanning tree instance. If you specify 0 (defined as the default CIST ID) as the mstid, you are configuring the common and internal spanning tree instance.

If the you specify cost, this command sets the path cost for this port within a multiple spanning tree instance or the common and internal spanning tree instance, depending on the mstid parameter, to the default value, that is, a path cost value based on the Link Speed.

If you specify port-priority, this command sets the priority for this port within a specific multiple spanning tree instance or the common and internal spanning tree instance, depending on the mstid parameter, to the default value.

Format	`no spanning-tree mst` *`mstid`* `{cost | port-priority}`
Mode	Interface Config

spanning-tree mst instance

This command adds a multiple spanning tree instance to the switch. The parameter mstid is a number within a range of 1 to 4094, that corresponds to the new instance ID to be added. The maximum number of multiple instances supported by the switch is 4.

Default	None
Format	`spanning-tree mst instance` *`mstid`*
Mode	Global Config

no spanning-tree mst instance

This command removes a multiple spanning tree instance from the switch and reallocates all VLANs allocated to the deleted instance to the common and internal spanning tree. The parameter mstid is a number that corresponds to the desired existing multiple spanning tree instance to be removed.

Format	`no spanning-tree mst instance` *`mstid`*
Mode	Global Config

spanning-tree mst priority

This command sets the bridge priority for a specific multiple spanning tree instance. The parameter mstid is a number that corresponds to the desired existing multiple spanning tree instance. The priority value is a number within a range of 0 to 4094.

If you specify 0 (defined as the default CIST ID) as the mstid, this command sets the Bridge Priority parameter to a new value for the common and internal spanning tree. The bridge priority value is a number within a range of 0 to 4094. The twelve least significant bits are masked according to the 802.1s specification. This causes the priority to be rounded down to the next lower valid priority.

Default	32768
Format	`spanning-tree mst priority` *`mstid 0`*`-4094`
Mode	Global Config

no spanning-tree mst priority

This command sets the bridge priority for a specific multiple spanning tree instance to the default value. The parameter mstid is a number that corresponds to the desired existing multiple spanning tree instance.

If 0 (defined as the default CIST ID) is passed as the mstid, this command sets the Bridge Priority parameter for the common and internal spanning tree to the default value.

Format	`no spanning-tree mst priority` *`mstid`*
Mode	Global Config

spanning-tree mst vlan

This command adds an association between a multiple spanning tree instance and one or more VLANs so that the VLAN(s) are no longer associated with the common and internal spanning tree. The parameter mstid is a multiple spanning tree instance identifier, in the range of 0 to 4094, that corresponds to the desired existing multiple spanning tree instance. The vlanid can be specified as a single VLAN, a list, or a range of values. To specify a list of VLANs, enter a list of VLAN IDs in the range 1 to 4093, each separated by a comma with no spaces in between. To specify a range of VLANs, separate the beginning and ending VLAN ID with a dash (-). Spaces and zeros are not permitted. The VLAN IDs may or may not exist in the system.

Format	`spanning-tree mst vlan` *`mstid vlanid`*
Mode	Global Config

no spanning-tree mst vlan

This command removes an association between a multiple spanning tree instance and one or more VLANs so that the VLAN(s) are again associated with the common and internal spanning tree.

Format	`no spanning-tree mst vlan` *`mstid vlanid`*
Mode	Global Config

spanning-tree port mode

This command sets the Administrative Switch Port State for this port to enabled for use by spanning tree.

Default	Enabled
Format	`spanning-tree port mode`
Mode	Interface Config

no spanning-tree port mode

This command sets the Administrative Switch Port State for this port to disabled, disabling the port for use by spanning tree.

Format	`no spanning-tree port mode`
Mode	Interface Config

spanning-tree port mode all

This command sets the Administrative Switch Port State for all ports to enabled.

Default	Enabled
Format	`spanning-tree port mode all`
Mode	Global Config

no spanning-tree port mode all

This command sets the Administrative Switch Port State for all ports to disabled.

Format	`no spanning-tree port mode all`
Mode	Global Config

spanning-tree port-priority

Use this command to change the priority value of the port to allow the operator to select the relative importance of the port in the forwarding process. Set this value to a lower number to prefer a port for forwarding of frames.

All LAN ports have 128 as priority value by default. PVSTP/PVRSTP puts the LAN port with the lowest LAN port number in the forwarding state and blocks other LAN ports.

The application uses the port priority value when the LAN port is configured as an edge port.

Default	Enabled
Format	`spanning-tree port-priority` *`0-240`*
Mode	Interface Config

spanning-tree tcnguard

Use this command to enable TCN guard on the interface. When enabled, TCN Guard restricts the interface from propagating any topology change information received through that interface.

Default	Enabled
Format	`spanning-tree tcnguard`
Mode	Interface Config

no spanning-tree tcnguard

This command resets the TCN guard status of the port to the default value.

Format	`no spanning-tree tcnguard`
Mode	Interface Config

spanning-tree transmit

This command sets the Bridge Transmit Hold Count parameter.

Default	6
Format	`spanning-tree transmit` *`hold-count`*
Mode	Global Config

Parameter	Description
`hold-count`	The Bridge Tx hold-count parameter. The value in an integer between 1 and 10.

spanning-tree uplinkfast

Use this command to configure the rate at which gratuitous frames are sent (in packets per second) after switchover to an alternate port on PVSTP configured switches and enables uplinkfast on PVSTP switches. The range is 0-32000; the default is 150. This command has the effect of accelerating spanning-tree convergence after switchover to an alternate port.

Uplinkfast can be configured even if the switch is configured for MST(RSTP) mode, but it only has an effect when the switch is configured for PVST mode. Enabling FastUplink increases the priority by 3000. Path costs less than 3000 have an additional 3000 added when uplinkfast is enabled. This reduces the probability that the switch will become the root switch.

Uplinkfast immediately changes to an alternate root port on detecting a root port failure and changes the new root port directly to the forwarding state. A TCN is sent for this event.

After a switchover to an alternate port (new root port), uplinkfast multicasts a gratuitous frame on the new root port on behalf of each attached machine so that the rest of the network knows to use the secondary link to reach that machine.

PVRSTP embeds support for backbonefast and uplinkfast. There is no provision to enable or disable these features in PVRSTP configured switches.

Default	150
Format	`spanning-tree uplinkfast [max-update-rate` *`packets`*`]`
Mode	Global Config

no spanning-tree uplinkfast

This command disables uplinkfast on PVSTP configured switches. All switch priorities and path costs that have not been modified from their default values are set to their default values.

Format	`no spanning-tree uplinkfast [max-update-rate]`
Mode	Global Config

spanning-tree vlan

Use this command to enable/disable spanning tree on a VLAN.

Default	None
Format	`spanning-tree vlan` *`vlan-list`*
Mode	Global Config

Parameter	Description
`vlan-list`	The VLANs to which to apply this command.

spanning-tree vlan cost

Use this command to set the path cost for a port in a VLAN. The valid values are in the range of 1 to 200000000 or auto. If auto is selected, the path cost value is set based on the link speed.

Default	None
Format	`spanning-tree vlan` *`vlan-id`* `cost {auto |`*`1-200000000`*`}`
Mode	Interface Config

spanning-tree vlan forward-time

Use this command to configure the spanning tree forward delay time for a VLAN or a set of VLANs. The default is 15 seconds.

Set this value to a lower number to accelerate the transition to forwarding. The network operator should take into account the end-to-end BPDU propagation delay, the maximum frame lifetime, the maximum transmission halt delay, and the message age overestimate values specific to their network when configuring this parameter.

Default	15 seconds
Format	`spanning-tree vlan` *`vlan-list`* `forward-time` *`4-30`*
Mode	Global Config

Parameter	Description
`vlan-list`	The VLANs to which to apply this command.
`forward-time`	The spanning tree forward delay time. The range is 4-30 seconds.

spanning-tree vlan hello-time

Use this command to configure the spanning tree hello time for a specified VLAN or a range of VLANs. The default is 2 seconds. Set this value to a lower number to accelerate the discovery of topology changes.

Default	2 seconds
Format	`spanning-tree vlan` *`vlan-list`* `hello-time` *`1-10`*
Mode	Global Config

Parameter	Description
`vlan-list`	The VLANs to which to apply this command.
`hello-time`	The spanning tree forward hello time. The range is 1-10 seconds.

spanning-tree vlan max-age

Use this command to configure the spanning tree maximum age time for a set of VLANs. The default is 20 seconds.

Set this value to a lower number to accelerate the discovery of topology changes. The network operator must take into account the end-to-end BPDU propagation delay and message age overestimate for their specific topology when configuring this value.

The default setting of 20 seconds is suitable for a network of diameter 7, lost message value of 3, transit delay of 1, hello interval of 2 seconds, overestimate per bridge of 1 second, and a BPDU delay of 1 second. For a network of diameter 4, a setting of 16 seconds is appropriate if all other timers remain at their default values.

Default	20 seconds
Format	`spanning-tree vlan` *`vlan-list`* `max-age` *`6-40`*
Mode	Global Config

Parameter	Description
vlan-list	The VLANs to which to apply this command.
max-age	The spanning tree forward hello time. The range is 1-10 seconds.

spanning-tree vlan root

Use this command to configure the switch to become the root bridge or standby root bridge by modifying the bridge priority from the default value of 32768 to a lower value calculated to ensure the bridge is the root (or standby) bridge.

The logic takes care of setting the bridge priority to a value lower (primary) or next lower (secondary) than the lowest bridge priority for the specified VLAN or a range of VLANs.

Default	32768
Format	`spanning-tree vlan vlan-list root {primary|secondary}`
Mode	Global Config

Parameter	Description
vlan-list	The VLANs to which to apply this command.

spanning-tree vlan port-priority

Use this command to change the VLAN port priority value of the VLAN port to allow the operator to select the relative importance of the VLAN port in the forwarding selection process when the port is configured as a point-to-point link type. Set this value to a lower number to prefer a port for forwarding of frames.

Default	None
Format	`spanning-tree vlan vlan-id port-priority priority`
Mode	Interface Config

Parameter	Description
vlan-list	The VLANs to which to apply this command.
priority	The VLAN port priority. The range is 0-255.

spanning-tree vlan priority

Use this command to configure the bridge priority of a VLAN. The default value is 32768.

If the value configured is not among the specified values, it will be rounded off to the nearest valid value.

Default	32768
Format	`spanning-tree vlan` *`vlan-list`* `priority` *`priority`*
Mode	Global Config

Parameter	Description
`vlan-list`	The VLANs to which to apply this command.
`priority`	The VLAN bridge priority. Valid values are 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440.

show spanning-tree

This command displays spanning tree settings for the common and internal spanning tree. The following details are displayed.

Format	`show spanning-tree`
Mode	• Privileged EXEC • User EXEC

Column	Meaning
Bridge Priority	Specifies the bridge priority for the Common and Internal Spanning tree (CST). The value lies between 0 and 61440. It is displayed in multiples of 4096.
Bridge Identifier	The bridge identifier for the CST. It is made up using the bridge priority and the base MAC address of the bridge.
Time Since Topology Change	Time in seconds.
Topology Change Count	Number of times changed.
Topology Change in Progress	Boolean value of the Topology Change parameter for the switch indicating if a topology change is in progress on any port assigned to the common and internal spanning tree.
Designated Root	The bridge identifier of the root bridge. It is made up from the bridge priority and the base MAC address of the bridge.
Root Path Cost	Value of the Root Path Cost parameter for the common and internal spanning tree.
Root Port Identifier	Identifier of the port to access the Designated Root for the CST
Bridge Max Age	Derived value.
Bridge Max Hops	Bridge max-hops count for the device.
Root Port Bridge Forward Delay	Derived value.
Hello Time	Configured value of the parameter for the CST.
Bridge Hold Time	Minimum time between transmission of Configuration Bridge Protocol Data Units (BPDUs).
CST Regional Root	Bridge Identifier of the CST Regional Root. It is made up using the bridge priority and the base MAC address of the bridge.
Regional Root Path Cost	Path Cost to the CST Regional Root.

Column	Meaning
Associated FIDs	List of forwarding database identifiers currently associated with this instance.
Associated VLANs	List of VLAN IDs currently associated with this instance.

The following example shows CLI display output for the command.

```
(Extreme 220) (Routing) #show spanning-tree
Bridge Priority..................................... 32768
Bridge Identifier................................... 80:00:00:10:18:48:FC:07
Time Since Topology Change.......................... 8 day 3 hr 22 min 37 sec
Topology Change Count............................... 0
Topology Change in progress........................ FALSE
Designated Root..................................... 80:00:00:10:18:48:FC:07
Root Path Cost...................................... 0
Root Port Identifier................................ 00:00
Bridge Max Age...................................... 20
Bridge Max Hops..................................... 20
Bridge Tx Hold Count................................ 6
Bridge Forwarding Delay............................. 15
Hello Time.......................................... 2
Bridge Hold Time.................................... 6
CST Regional Root................................... 80:00:00:10:18:48:FC:07
Regional Root Path Cost............................. 0
     Associated FIDs           Associated VLANs
     ---------------           ----------------
(Extreme 220) (Routing) #
```

show spanning-tree active

Use this command to display the spanning tree values on active ports for the modes (xSTP and PV(R)STP).

Format	`show spanning-tree active`
Mode	• Privileged EXEC • User EXEC

Example 1

```
(Extreme 220) (Routing)#show spanning-tree active
Spanning Tree: Enabled (BPDU Flooding: Disabled) Portfast BPDU Filtering: Disabled
Mode: rstp
CST Regional Root:        80:00:00:01:85:48:F0:0F
Regional Root Path Cost:  0
###### MST 0 Vlan Mapped:   3
ROOT ID
             Priority        32768
             Address         00:00:EE:EE:EE:EE
             This Switch is the Root.
             Hello Time: 2s Max Age: 20s Forward Delay: 15s
Interfaces
Name      State    Prio.Nbr  Cost      Sts           Role  RestrictedPort
--------- -------- --------- --------- ------------- ----- --------------
0/49      Enabled  128.49    2000      Forwarding    Desg  No
3/1       Enabled  96.66     5000      Forwarding    Desg  No
3/2       Enabled  96.67     5000      Forwarding    Desg  No
3/10      Enabled  96.75     0         Forwarding    Desg  No
```

Example 2

```
(Extreme 220) (Routing)#show spanning-tree active
Spanning-tree enabled protocol rpvst
VLAN    1
 RootID    Priority        32769
           Address         00:00:EE:EE:EE:EE
           Cost            0
           Port            This switch is the root
           Hello Time 2 Sec Max Age 20 sec Forward Delay 15 sec
 BridgeID  Priority        32769 (priority 32768 sys-id-ext 1)
           Address         00:00:EE:EE:EE:EE
           Hello Time 2 Sec Max Age 20 sec Forward Delay 15 sec
           Aging Time 300 sec
Interface State     Prio.Nbr  Cost    Status        Role
--------- --------- --------- ------- ------------- -----------
0/49      Enabled   128.49    2000    Forwarding    Designated
3/1       Enabled   128.66    5000    Forwarding    Designated
3/2       Enabled   128.67    5000    Forwarding    Designated
3/10      Enabled   128.75    0       Forwarding    Designated
VLAN    3
 RootID    Priority        32771
           Address         00:00:EE:EE:EE:EE
           Cost            0
           Port            This switch is the root
           Hello Time 2 Sec Max Age 20 sec Forward Delay 15 sec
 BridgeID  Priority        32771 (priority 32768 sys-id-ext 3)
           Address         00:00:EE:EE:EE:EE
           Hello Time 2 Sec Max Age 20 sec Forward Delay 15 sec
           Aging Time 300 sec
Interface State     Prio.Nbr  Cost    Status        Role
--------- --------- --------- ------- ------------- -----------
3/1       Enabled   128.66    5000    Forwarding    Designated
3/2       Enabled   128.67    5000    Forwarding    Designated
3/10      Enabled   128.75    0       Forwarding    Designated
```

Example 3

```
(Extreme 220) (Routing)#show spanning-tree active
Spanning-tree enabled protocol rpvst
VLAN    1
 RootID    Priority        32769
           Address         00:00:EE:EE:EE:EE
           Cost            0
           Port            10(3/10   )
           Hello Time 2 Sec Max Age 20 sec Forward Delay 15 sec
 BridgeID  Priority        32769 (priority 32768 sys-id-ext 1)
           Address         00:00:EE:EE:EE:EE
           Hello Time 2 Sec Max Age 20 sec Forward Delay 15 sec
           Aging Time 300 sec
Interface State     Prio.Nbr  Cost    Status        Role
--------- --------- --------- ------- ------------- -----------
0/49      Enabled   128.49    2000    Discarding    Alternate
3/1       Enabled   128.66    5000    Forwarding    Disabled
3/2       Enabled   128.67    5000    Forwarding    Disabled
3/10      Enabled   128.75    0       Forwarding    Root
VLAN    3
 RootID    Priority        32771
           Address         00:00:EE:EE:EE:EE
           Cost            0
           Port            10(3/10   )
           Hello Time 2 Sec Max Age 20 sec Forward Delay 15 sec
 BridgeID  Priority        32771 (priority 32768 sys-id-ext 3)
           Address         00:00:EE:EE:EE:EE
```

```
           Hello Time 2 Sec Max Age 20 sec Forward Delay 15 sec
           Aging Time 300 sec
Interface State     Prio.Nbr  Cost    Status        Role
--------- --------- --------- ------- ------------- -----------
3/1       Enabled   128.66    5000    Forwarding    Disabled
3/2       Enabled   128.67    5000    Forwarding    Disabled
3/10      Enabled   128.75    0       Forwarding    Root
```

show spanning-tree backbonefast

This command displays spanning tree information for backbonefast.

Format	`show spanning-tree backbonefast`
Mode	• Privileged EXEC • User EXEC

Column	Meaning
Transitions via Backbonefast	The number of backbonefast transitions.
Inferior BPDUs received (all VLANs)	The number of inferior BPDUs received on all VLANs.
RLQ request PDUs received (all VLANs)	The number of root link query (RLQ) requests PDUs received on all VLANs.
RLQ response PDUs received (all VLANs)	The number of RLQ response PDUs received on all VLANs.
RLQ request PDUs sent (all VLANs)	The number of RLQ request PDUs sent on all VLANs.
RLQ response PDUs sent (all VLANs)	The number of RLQ response PDUs sent on all VLANs.

The following example shows output from the command.

```
(Extreme 220) (Routing)#show spanning-tree backbonefast
Backbonefast Statistics
-----------------------
Transitions via Backbonefast (all VLANs)          : 0
Inferior BPDUs received (all VLANs)               : 0
RLQ request PDUs received (all VLANs)             : 0
RLQ response PDUs received (all VLANs)            : 0
RLQ request PDUs sent (all VLANs)                 : 0
RLQ response PDUs sent (all VLANs)                : 0
```

show spanning-tree brief

This command displays spanning tree settings for the bridge. The following information appears.

Format	`show spanning-tree brief`
Mode	• Privileged EXEC • User EXEC

Column	Meaning
Bridge Priority	Configured value.

Column	Meaning
Bridge Identifier	The bridge identifier for the selected MST instance. It is made up using the bridge priority and the base MAC address of the bridge.
Bridge Max Age	Configured value.
Bridge Max Hops	Bridge max-hops count for the device.
Bridge Hello Time	Configured value.
Bridge Forward Delay	Configured value.
Bridge Hold Time	Minimum time between transmission of Configuration Bridge Protocol Data Units (BPDUs).

The following example shows CLI display output for the command.

```
(Extreme 220) (Routing) #show spanning-tree brief
Bridge Priority.............................. 32768
Bridge Identifier............................ 80:00:00:10:18:48:FC:07
Bridge Max Age............................... 20
Bridge Max Hops.............................. 20
Bridge Hello Time............................ 2
Bridge Forward Delay......................... 15
Bridge Hold Time............................. 6
(Extreme 220) (Routing) #
```

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 is the desired switch port. 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. The following details are displayed on execution of the command.

Format	`show spanning-tree interface` *`unit/slot/port`*`|lag lag-intf-num`
Mode	• Privileged EXEC • User EXEC

Column	Meaning
Hello Time	Admin hello time for this port.
Port Mode	Enabled or disabled.
BPDU Guard Effect	Enabled or disabled.
Root Guard	Enabled or disabled.
Loop Guard	Enabled or disabled.
TCN Guard	Enable or disable the propagation of received topology change notifications and topology changes to other ports.
BPDU Filter Mode	Enabled or disabled.
BPDU Flood Mode	Enabled or disabled.
Auto Edge	To enable or disable the feature that causes a port that has not seen a BPDU for edge delay time, to become an edge port and transition to forwarding faster.

Column	Meaning
Port Up Time Since Counters Last Cleared	Time since port was reset, displayed in days, hours, minutes, and seconds.
STP BPDUs Transmitted	Spanning Tree Protocol Bridge Protocol Data Units sent.
STP BPDUs Received	Spanning Tree Protocol Bridge Protocol Data Units received.
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	*MSTP* Bridge Protocol Data Units sent.
MSTP BPDUs Received	Multiple Spanning Tree Protocol Bridge Protocol Data Units received.

The following example shows CLI display output for the command.

```
(Extreme 220) (Routing) #show spanning-tree interface 0/1
Hello Time..................................... Not Configured
Port Mode...................................... Enabled
BPDU Guard Effect.............................. Disabled
Root Guard..................................... FALSE
Loop Guard..................................... FALSE
TCN Guard...................................... FALSE
BPDU Filter Mode............................... Disabled
BPDU Flood Mode................................ Disabled
Auto Edge...................................... TRUE
Port Up Time Since Counters Last Cleared....... 8 day 3 hr 39 min 58 sec
STP BPDUs Transmitted.......................... 0
STP BPDUs Received............................. 0
RSTP BPDUs Transmitted......................... 0
RSTP BPDUs Received............................ 0
MSTP BPDUs Transmitted......................... 0
MSTP BPDUs Received............................ 0
(Extreme 220) (Routing) #
```

The following example shows CLI display output for the command.

```
(Extreme 220) (Routing) #show spanning-tree interface lag 1
Hello Time..................................... Not Configured
Port Mode...................................... Enabled
BPDU Guard Effect.............................. Disabled
Root Guard..................................... FALSE
Loop Guard..................................... FALSE
TCN Guard...................................... FALSE
BPDU Filter Mode............................... Disabled
BPDU Flood Mode................................ Disabled
Auto Edge...................................... TRUE
Port Up Time Since Counters Last Cleared....... 8 day 3 hr 42 min 5 sec
STP BPDUs Transmitted.......................... 0
STP BPDUs Received............................. 0
RSTP BPDUs Transmitted......................... 0
RSTP BPDUs Received............................ 0
MSTP BPDUs Transmitted......................... 0
MSTP BPDUs Received............................ 0
(Extreme 220) (Routing) #
```

show spanning-tree mst detailed

This command displays the detailed settings for an MST instance.

Format	`show spanning-tree mst detailed` *mstid*
Mode	• Privileged EXEC • User EXEC

Parameter	Description
mstid	A multiple spanning tree instance identifier. The value is 0–4094.

The following example shows CLI display output for the command.

```
(Extreme 220) (Routing) #show spanning-tree mst detailed 0
MST Instance ID............................... 0
MST Bridge Priority........................... 32768
MST Bridge Identifier......................... 80:00:00:10:18:48:FC:07
Time Since Topology Change.................... 8 day 3 hr 47 min 7 sec
Topology Change Count......................... 0
Topology Change in progress................... FALSE
Designated Root............................... 80:00:00:10:18:48:FC:07
Root Path Cost................................ 0
Root Port Identifier.......................... 00:00
     Associated FIDs           Associated VLANs
     ---------------           ----------------
(Extreme 220) (Routing) #
```

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 is the desired switch port. 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.

Format	`show spanning-tree mst port detailed` *mstid unit/slot/port*`|lag lag-intf-num`
Mode	• Privileged EXEC • User EXEC

Column	Meaning
MST Instance ID	The ID of the existing multiple spanning tree (MST) instance identifier. The value is 0–4094.
Port Identifier	The port identifier for the specified port within the selected MST instance. It is made up from the port priority and the interface number of the port.
Port Priority	The priority for a particular port within the selected MST instance. The port priority is displayed in multiples of 16.
Port Forwarding State	Current spanning tree state of this port.
Port Role	Each enabled MST Bridge Port receives a Port Role for each spanning tree. The port role is one of the following values: Root Port, Designated Port, Alternate Port, Backup Port, Master Port or Disabled Port

Column	Meaning
Auto-Calculate Port Path Cost	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.

Column	Meaning
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	Whether auto calculation for port path cost is enabled or not (disabled).
Port Path Cost	The configured path cost for the specified interface.
Auto-Calculate External Port Path Cost	Whether auto calculation for external port path cost is enabled.
External Port Path Cost	The cost to get to the root bridge of the CIST across the boundary of the region. This means that if the port is a boundary port for an *MSTP* region, then the external path cost is used.
Designated Root	Identifier of the designated root for this port within the CST.
Root Path Cost	The root path cost to the LAN by the port.
Designated Bridge	The bridge containing the designated port.
Designated Port Identifier	Port on the Designated Bridge that offers the lowest cost to the LAN.
Topology Change Acknowledgment	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.

Column	Meaning
Point To Point MAC Status	Derived value indicating if this port is part of a point to point link.
CST Regional Root	The regional root identifier in use for this port.
CST Internal Root Path Cost	The internal root path cost to the LAN by the designated external port.
Loop Inconsistent State	The current loop inconsistent state of this port in this MST instance. When in loop inconsistent state, the port has failed to receive BPDUs while configured with loop guard enabled. Loop inconsistent state maintains the port in a blocking state until a subsequent BPDU is received.
Transitions Into Loop Inconsistent State	The number of times this interface has transitioned into loop inconsistent state.
Transitions Out of Loop Inconsistent State	The number of times this interface has transitioned out of loop inconsistent state.

The following example shows CLI display output for the command in slot/port format.

```
(Extreme 220) (Routing) #show spanning-tree mst port detailed 0 0/1
Port Identifier.............................. 80:01
Port Priority................................ 128
Port Forwarding State........................ Disabled
Port Role.................................... Disabled
Auto-calculate Port Path Cost................ Enabled
Port Path Cost............................... 0
Auto-Calculate External Port Path Cost....... Enabled
External Port Path Cost...................... 0
Designated Root.............................. 80:00:00:10:18:48:FC:07
Root Path Cost............................... 0
Designated Bridge............................ 80:00:00:10:18:48:FC:07
Designated Port Identifier................... 00:00
Topology Change Acknowledge.................. FALSE
Hello Time................................... 2
Edge Port.................................... FALSE
Edge Port Status............................. FALSE
Point to Point MAC Status.................... TRUE
CST Regional Root............................ 80:00:00:10:18:48:FC:07
CST Internal Root Path Cost.................. 0
Loop Inconsistent State...................... FALSE
Transitions Into Loop Inconsistent State..... 0
Transitions Out Of Loop Inconsistent State..... 0
```

The following example shows CLI display output for the command using a LAG interface number.

```
(Extreme 220) (Routing) #show spanning-tree mst port detailed 0 lag 1
Port Identifier.............................. 60:42
Port Priority................................ 96
Port Forwarding State........................ Disabled
Port Role.................................... Disabled
Auto-calculate Port Path Cost................ Enabled
Port Path Cost............................... 0
Auto-Calculate External Port Path Cost....... Enabled
External Port Path Cost...................... 0
Designated Root.............................. 80:00:00:10:18:48:FC:07
Root Path Cost............................... 0
Designated Bridge............................ 80:00:00:10:18:48:FC:07
Designated Port Identifier................... 00:00
Topology Change Acknowledge.................. FALSE
Hello Time................................... 2
Edge Port.................................... FALSE
Edge Port Status............................. FALSE
```

```
Point to Point MAC Status..................... TRUE
CST Regional Root............................. 80:00:00:10:18:48:FC:07
CST Internal Root Path Cost................... 0
Loop Inconsistent State....................... FALSE
Transitions Into Loop Inconsistent State...... 0
Transitions Out Of Loop Inconsistent State..... 0
--More-- or (q)uit
(Extreme 220) (Routing) #
```

show spanning-tree mst port summary

This command displays the settings of one or all ports within the specified multiple spanning tree instance. The parameter mstid indicates a particular MST instance. The parameter {unit/slot/port|all} indicates the desired switch port or all ports. 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.

If you specify 0 (defined as the default CIST ID) as the mstid, the status summary displays for one or all ports within the common and internal spanning tree.

Format	`show spanning-tree mst port summary` *`mstid`* {*`unit/slot/port`* | `lag` *`lag-intf-num`*| `all`}
Mode	• Privileged EXEC • User EXEC

Column	Meaning
MST Instance ID	The MST instance associated with this port.
Interface	*unit/slot/port*
STP Mode	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	Whether the port is in loop inconsistent state or not. This field is blank if the loop guard feature is not available.

The following example shows CLI display output for the command in slot/port format.

```
(Extreme 220) (Routing) #show spanning-tree mst port summary 0 0/1
MST Instance ID............................... CST
            STP                  STP            Port
Interface   Mode   Type          State          Role       Desc
--------- -------- ------- ----------------- ---------- ----------
0/1       Enabled          Disabled          Disabled
```

The following example shows CLI display output for the command using a LAG interface number.

```
(Extreme 220) (Routing) #show spanning-tree mst port summary 0 lag 1
MST Instance ID............................... CST
            STP                  STP            Port
Interface   Mode   Type          State          Role       Desc
--------- -------- ------- ----------------- ---------- ----------
3/1       Enabled          Disabled          Disabled
```

show spanning-tree mst port summary active

This command displays settings for the ports within the specified multiple spanning tree instance that are active links.

Format	`show spanning-tree mst port summary` *`mstid`* `active`
Mode	• Privileged EXEC • User EXEC

Column	Meaning
MST Instance ID	The ID of the existing MST instance.
Interface	*unit/slot/port*
STP Mode	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	Whether the port is in loop inconsistent state or not. This field is blank if the loop guard feature is not available.

The following example shows CLI display output for the command.

```
(Extreme 220) (Routing) >show spanning-tree mst port summary 0 active
            STP                  STP            Port
Interface   Mode   Type         State           Role       Desc
--------- -------- ------- ----------------- ---------- ---------
```

show spanning-tree mst summary

This command displays summary information about all multiple spanning tree instances in the switch. On execution, the following details are displayed.

Format	`show spanning-tree mst summary`
Mode	• Privileged EXEC • User EXEC

Column	Meaning
MST Instance ID List	List of multiple spanning trees IDs currently configured.
For each MSTID:Associated FIDsAssociated VLANs	• List of forwarding database identifiers associated with this instance. • List of VLAN IDs associated with this instance.

show spanning-tree summary

This command displays spanning tree settings and parameters for the switch. The following details are displayed on execution of the command.

Format	`show spanning-tree summary`
Mode	• Privileged EXEC • User EXEC

Column	Meaning
Spanning Tree Adminmode	Enabled or disabled.
Spanning Tree Version	Version of 802.1 currently supported (IEEE 802.1s, IEEE 802.1w, or IEEE 802.1d) based upon the Force Protocol Version parameter.
BPDU Guard Mode	Enabled or disabled.
BPDU Filter Mode	Enabled or disabled.
Configuration Name	Identifier used to identify the configuration currently being used.
Configuration Revision Level	Identifier used to identify the configuration currently being used.
Configuration Digest Key	A generated Key used in the exchange of the BPDUs.
Configuration Format Selector	Specifies the version of the configuration format being used in the exchange of BPDUs. The default value is zero.
MST Instances	List of all multiple spanning tree instances configured on the switch.

The following example shows CLI display output for the command.

```
(Extreme 220) (Routing) #show spanning-tree summary
Spanning Tree Adminmode.......... Enabled
Spanning Tree Version............ IEEE 802.1s
BPDU Guard Mode.................. Disabled
BPDU Filter Mode................. Disabled
Configuration Name............... ****
Configuration Revision Level..... ****
Configuration Digest Key......... ****
Configuration Format Selector..... 0
No MST instances to display.
```

show spanning-tree uplinkfast

This command displays spanning tree information for uplinkfast.

Format	`show spanning-tree uplinkfast`
Mode	• Privileged EXEC • User EXEC

Column	Meaning
Uplinkfast transitions (all VLANs)	The number of uplinkfast transitions on all VLANs.
Proxy multicast addresses transmitted (all VLANs)	The number of proxy multicast addresses transmitted on all VLANs.

The following example shows output from the command.

```
(Extreme 220) (Routing) #show spanning-tree uplinkfast
Uplinkfast is enabled.
BPDU update rate : 150 packets/sec
Uplinkfast Statistics
---------------------
Uplinkfast transitions (all VLANs)................. 0
Proxy multicast addresses transmitted (all VLANs).. 0
```

show spanning-tree vlan

This command displays spanning tree information per VLAN and also lists out the port roles and states along with port cost. The vlan-list parameter is a list of VLANs or VLAN-ranges separated by commas and with no embedded blank spaces. VLAN ranges are of the form “X-Y” where X and Y are valid VLAN identifiers and X< Y. The vlanid corresponds to an existing VLAN ID.

Format	`show spanning-tree vlan {`*`vlanid`* `|` *`vlan-list`*`}`
Mode	• Privileged EXEC • User EXEC

The following example shows CLI display output for the command.

```
(Extreme 220) (Routing) #show spanning-tree vlan 1
VLAN    1
          Spanning-tree enabled protocol rpvst
          RootID    Priority        32769
           Address         00:0C:29:D3:80:EA
           Cost            0
           Port            This switch is the root
           Hello Time 2 Sec Max Age 15 sec Forward Delay 15 sec
 BridgeID  Priority        32769 (priority 32768 sys-id-ext 1)
           Address         00:0C:29:D3:80:EA
           Hello Time 2 Sec Max Age 15 sec Forward Delay 15 sec
           Aging Time 300
Interface  Role        Sts            Cost         Prio.Nbr
---------  ----------  -------------  ---------    --------
1/0/1      Designated  Forwarding     3000        128.1
1/0/2      Designated  Forwarding     3000        128.2
1/0/3      Disabled    Disabled       3000        128.3
1/0/4      Designated  Forwarding     3000        128.4
1/0/5      Designated  Forwarding     3000        128.5
1/0/6      Designated  Forwarding     3000        128.6
1/0/7      Designated  Forwarding     3000        128.7
1/0/8      Designated  Forwarding     3000        128.8
0/1/1      Disabled    Disabled       3000        128.1026
0/1/2      Disabled    Disabled       3000        128.1027
0/1/3      Disabled    Disabled       3000        128.1028
0/1/4      Disabled    Disabled       3000        128.1029
0/1/5      Disabled    Disabled       3000        128.1030
0/1/6      Disabled    Disabled       3000        128.1031
```

Loop Protection Commands

This section describes the commands used to configure loop protection. Loop protection detects physical and logical loops between Ethernet ports on a device. Loop protection must be enabled globally before it can be enabled at the interface level.

keepalive (Global Config)

This command enables loop protection for the system.

Default	Disabled
Format	`keepalive`
Mode	Global Config

no keepalive

This command disables loop protection for the system. This command also sets the transmit interval and retry count to the default value.

Format	`no keepalive`
Mode	Global Config

keepalive (Interface Config)

This command enables keepalive on a particular interface.

Default	None
Format	`keepalive`
Mode	Interface Config

no keepalive

This command disables keepalive on a particular interface.

Format	`no keepalive`
Mode	Interface Config

keepalive action

This command configures the action to be taken on a port when a loop is detected.

Default	Disabled.
Format	`keepalive receive-action {log|disable|both}`
Mode	Interface Configuration

Parameter	Description
log	Only logs the message. The log mode only logs the message to buffer logs without bringing the port down.
disable	Shuts down the port. This is the default.
both	Logs and disables the port.

no keepalive action

This command returns the command to the default action of disabling a port when a loop is detected.

Format	`no keepalive receive-action {log|disable|both}`
Mode	Interface Configuration

keepalive disable-timer

This command configures the time, in seconds, for which a port is down if a loop is detected. The default time is 0 so that port needs to be re-enabled manually to bring it up.

Default	0
Format	`keep-alive disable-timer` *`value`*
Mode	Global Configuration

Parameter	Description
`value`	The time, in seconds, for which the port is down if a loop is detected.

no keepalive disable-timer

This command removes the disable-timer.

Format	`no keep-alive disable-timer`
Mode	Global Configuration

keepalive retry

This command configures the time in seconds between transmission of keep-alive packets. Retry is an optional parameter that configures the count of keepalive packets received by the switch after which the interface will be error disabled.

Default	5
Format	`keepalive val [retry]`
Mode	Global Configuration

Parameter	Description
val	The time in seconds between transmission of keep-alive packets.
retry	Configures the count of keepalive packets received by the switch after which the switch will be error disabled.

show keepalive

This command displays the global keepalive configuration.

Default	None
Format	`show keepalive`
Mode	Privileged EXEC

```
(Extreme 220) (Routing) #show  keepalive
Keepalive          : Enabled
Transmit interval : 5 seconds
Retry count        : 1
```

show keepalive statistics

This command displays the keepalive statistics for each port or a specific port.

Default	None
Format	`show keepalive statistics {port-num | all }`
Mode	Privileged EXEC

Parameter	Definition
port-num	The port number for which to show statistics.
all	Show statistics for all ports.

```
(Extreme 220) (Routing) #show keepalive statistics all
       Keep      Loop        Loop     Time Since      Rx           Port
Port   Alive     Detected    Count    Last Loop     Action        Status
------ --------- ----------- -------- ------------- ------------- --------
0/1    Yes       Yes         1        85            shut-down     D-Disable
0/3    Yes       No                                 log-shutdown  Enable
```

clear counters keepalive

This command clears keepalive statistics associated with ports (for example, number of transmitted packets, received packets, and loop packets).

Default	None
Format	`clear counters keepalive`
Mode	Privileged EXEC

VLAN Commands

This section describes the commands used to configure VLAN settings.

vlan database

This command gives you access to the VLAN Config mode, which allows you to configure VLAN characteristics

Format	`vlan database`
Mode	Privileged EXEC

network mgmt_vlan

This command configures the Management VLAN ID.

Default	1
Format	`network mgmt_vlan` *`1-4093`*
Mode	Privileged EXEC

no network mgmt_vlan

This command sets the Management VLAN ID to the default.

Format	`no network mgmt_vlan`
Mode	Privileged EXEC

vlan

This command creates a new VLAN and assigns it an ID. The ID is a valid VLAN identification number (ID 1 is reserved for the default VLAN). VLAN range is 2-4093.

Format	`vlan` *`2-4093`*
Mode	VLAN Config

no vlan

This command deletes an existing VLAN. The ID is a valid VLAN identification number (ID 1 is reserved for the default VLAN). The VLAN range is 2-4093.

Format	`no vlan 2-4093`
Mode	VLAN Config

vlan acceptframe

This command sets the frame acceptance mode on an interface or range of interfaces. For VLAN Only mode, untagged frames or priority frames received on this interface are discarded. For Admit All mode, untagged frames or priority frames received on this interface are accepted and assigned the value of the interface VLAN ID for this port. For admituntaggedonly mode, only untagged frames are accepted on this interface; tagged frames are discarded. With any option, VLAN tagged frames are forwarded in accordance with the IEEE 802.1Q VLAN Specification.

Default	all
Format	`vlan acceptframe {admituntaggedonly | vlanonly | all}`
Mode	Interface Config

no vlan acceptframe

This command resets the frame acceptance mode for the interface or range of interfaces to the default value.

Format	`no vlan acceptframe`
Mode	Interface Config

vlan ingressfilter

This command enables ingress filtering on an interface or range of interfaces.

If ingress filtering is enabled, frames received with VLAN IDs that do not match the VLAN membership of the receiving interface are discarded.

If ingress filtering is disabled, frames received with VLAN IDs that do not match the VLAN membership of the receiving interface are admitted and forwarded to ports that are members of that VLAN.

Default	Disabled
Format	`vlan ingressfilter`
Mode	Interface Config

no vlan ingressfilter

This command disables ingress filtering.

If ingress filtering is disabled, frames received with VLAN IDs that do not match the VLAN membership of the receiving interface are admitted and forwarded to ports that are members of that VLAN.

If ingress filtering is enabled, frames received with VLAN IDs that do not match the VLAN membership of the receiving interface are discarded

Format	`no vlan ingressfilter`
Mode	Interface Config

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.

Format	`vlan internal allocation {base` *`vlan-id`* `| policy ascending | policy descending}`
Mode	Global Config

Parameter	Description
`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

vlan makestatic

This command changes a dynamically created VLAN (created by GVRP registration) to a static VLAN (one that is permanently configured and defined). The ID is a valid VLAN identification number. VLAN range is 2-4093.

Format	`vlan makestatic` *`2-4093`*
Mode	VLAN Config

vlan name

This command changes the name of a VLAN. The name is an alphanumeric string of up to 32 characters, and the ID is a valid VLAN identification number. ID range is 1-4093.

Default	• VLAN ID 1 - default • other VLANS - blank string
Format	`vlan name 1-4093 name`
Mode	VLAN Config

no vlan name

This command sets the name of a VLAN to a blank string.

Format	`no vlan name 1-4093`
Mode	VLAN Config

vlan participation

This command configures the degree of participation for a specific interface or range of interfaces in a VLAN. The ID is a valid VLAN identification number, and the interface is a valid interface number.

Format	`vlan participation {exclude | include | auto} 1-4093`
Mode	Interface Config

Participation options are:

Parameter	Description
include	The interface is always a member of this VLAN. This is equivalent to registration fixed.
exclude	The interface is never a member of this VLAN. This is equivalent to registration forbidden.
auto	The interface is dynamically registered in this VLAN by GVRP and will not participate in this VLAN unless a join request is received on this interface. This is equivalent to registration normal.

vlan participation all

This command configures the degree of participation for all interfaces in a VLAN. The ID is a valid VLAN identification number.

Format	`vlan participation all {exclude | include | auto} 1-4093`
Mode	Global Config

You can use the following participation options:

Parameter	Description
include	The interface is always a member of this VLAN. This is equivalent to registration fixed.
exclude	The interface is never a member of this VLAN. This is equivalent to registration forbidden.
auto	The interface is dynamically registered in this VLAN by GVRP. The interface will not participate in this VLAN unless a join request is received on this interface. This is equivalent to registration normal.

vlan port acceptframe all

This command sets the frame acceptance mode for all interfaces.

Default	all
Format	`vlan port acceptframe all {vlanonly | admituntaggedonly |all}`
Mode	Global Config

The modes are defined as follows:

Parameter	Description
vlanonly	Untagged frames or priority frames received on this interface are discarded.
admituntaggedonly	VLAN-tagged and priority tagged frames received on this interface are discarded.
all	Untagged frames or priority frames received on this interface are accepted and assigned the value of the interface VLAN ID for this port.

With either option, VLAN tagged frames are forwarded in accordance with the IEEE 802.1Q VLAN Specification.

no vlan port acceptframe all

This command sets the frame acceptance mode for all interfaces to Admit All. For Admit All mode, untagged frames or priority frames received on this interface are accepted and assigned the value of the interface VLAN ID for this port. With either option, VLAN tagged frames are forwarded in accordance with the IEEE 802.1Q VLAN Specification.

Format	`no vlan port acceptframe all`
Mode	Global Config

vlan port ingressfilter all

This command enables ingress filtering for all ports.

If ingress filtering is enabled, frames received with VLAN IDs that do not match the VLAN membership of the receiving interface are discarded

If ingress filtering is disabled, frames received with VLAN IDs that do not match the VLAN membership of the receiving interface are admitted and forwarded to ports that are members of that VLAN.

Default	Disabled
Format	`vlan port ingressfilter all`
Mode	Global Config

no vlan port ingressfilter all

This command disables ingress filtering for all ports.

If ingress filtering is disabled, frames received with VLAN IDs that do not match the VLAN membership of the receiving interface are admitted and forwarded to ports that are members of that VLAN.

If ingress filtering is enabled, frames received with VLAN IDs that do not match the VLAN membership of the receiving interface are discarded

Format	`no vlan port ingressfilter all`
Mode	Global Config

vlan port pvid all

This command changes the VLAN ID for all interface.

Default	1
Format	`vlan port pvid all` *`1-4093`*
Mode	Global Config

no vlan port pvid all

This command sets the VLAN ID for all interfaces to 1.

Format	`no vlan port pvid all`
Mode	Global Config

vlan port tagging all

This command configures the tagging behavior for all interfaces in a VLAN to enabled. If tagging is enabled, traffic is transmitted as tagged frames. If tagging is disabled, traffic is transmitted as untagged frames. The ID is a valid VLAN identification number.

Format	`vlan port tagging all` *`1-4093`*
Mode	Global Config

no vlan port tagging all

This command configures the tagging behavior for all interfaces in a VLAN to disabled. If tagging is disabled, traffic is transmitted as untagged frames. The ID is a valid VLAN identification number.

Format	`no vlan port tagging all`
Mode	Global Config

vlan protocol group

This command adds protocol-based VLAN groups to the system. The groupid is a unique number from 1–128 that is used to identify the group in subsequent commands.

Format	`vlan protocol group` *`groupid`*
Mode	Global Config

vlan protocol group name

This command assigns a name to a protocol-based VLAN groups. The groupname variable can be a character string of 0 to 16 characters.

Format	`vlan protocol group name` *`groupid groupname`*
Mode	Global Config

no vlan protocol group name

This command removes the name from the group identified by groupid.

Format	`no vlan protocol group name` *`groupid`*
Mode	Global Config

vlan protocol group add protocol

This command adds the protocol to the protocol-based VLAN identified by groupid. A group may have more than one protocol associated with it. Each interface and protocol combination can only be associated with one group. If adding a protocol to a group causes any conflicts with interfaces currently associated with the group, this command fails and the protocol is not added to the group. The possible values for protocol are The possible values for protocol-list includes the keywords ip, arp, and ipx and hexadecimal or decimal values ranging from 0x0600 (1536) to 0xFFFF (65535). The protocol list can accept up to 16 protocols separated by a comma.

Default	None
Format	`vlan protocol group add protocol` *`groupid ethertype protocol-list`*
Mode	Global Config

no vlan protocol group add protocol

This command removes the protocols specified in the protocol-list from this protocol-based VLAN group that is identified by this groupid.

Format	`no vlan protocol group add protocol` *`groupid ethertype protocol-list`*
Mode	Global Config

protocol group

This command attaches a vlanid to the protocol-based VLAN identified by groupid. A group may only be associated with one VLAN at a time, however the VLAN association can be changed.

Default	None
Format	`protocol group` *`groupid vlanid`*
Mode	VLAN Config

no protocol group

This command removes the vlanid from this protocol-based VLAN group that is identified by this groupid.

Format	`no protocol group` *`groupid vlanid`*
Mode	VLAN Config

protocol vlan group

This command adds a physical interface or a range of interfaces to the protocol-based VLAN identified by groupid. You can associate multiple interfaces with a group, but you can only associate each interface and protocol combination with one group. If adding an interface to a group causes any conflicts with protocols currently associated with the group, this command fails and the interface(s) are not added to the group.

Default	None
Format	`protocol vlan group` *`groupid`*
Mode	Interface Config

no protocol vlan group

This command removes the interface from this protocol-based VLAN group that is identified by this groupid.

Format	`no protocol vlan group` *`groupid`*
Mode	Interface Config

protocol vlan group all

This command adds all physical interfaces to the protocol-based VLAN identified by groupid. You can associate multiple interfaces with a group, but you can only associate each interface and protocol combination with one group. If adding an interface to a group causes any conflicts with protocols currently associated with the group, this command will fail and the interface(s) will not be added to the group.

Default	None
Format	`protocol vlan group all` *`groupid`*
Mode	Global Config

no protocol vlan group all

This command removes all interfaces from this protocol-based VLAN group that is identified by this groupid.

Format	`no protocol vlan group all` *`groupid`*
Mode	Global Config

show port protocol

This command displays the Protocol-Based VLAN information for either the entire system, or for the indicated group.

Format	`show port protocol {`*`groupid`* `| all}`
Mode	Privileged EXEC

Column	Meaning
Group Name	The group name of an entry in the Protocol-based VLAN table.
Group ID	The group identifier of the protocol group.
VLAN	The VLAN associated with this Protocol Group.
Protocol(s)	The type of protocol(s) for this group.
Interface(s)	Lists the *`unit/slot/port`* interface(s) that are associated with this Protocol Group.

vlan pvid

This command changes the VLAN ID on an interface or range of interfaces.

Default	1
Format	`vlan pvid 1-4093`
Mode	Interface Config Interface Range Config

no vlan pvid

This command sets the VLAN ID on an interface or range of interfaces to 1.

Format	`no vlan pvid`
Mode	Interface Config

vlan tagging

This command configures the tagging behavior for a specific interface or range of interfaces in a VLAN to enabled. If tagging is enabled, traffic is transmitted as tagged frames. If tagging is disabled, traffic is transmitted as untagged frames. The ID is a valid VLAN identification number.

Format	`vlan tagging 1-4093`
Mode	• Interface Config

no vlan tagging

This command configures the tagging behavior for a specific interface or range of interfaces in a VLAN to disabled. If tagging is disabled, traffic is transmitted as untagged frames. The ID is a valid VLAN identification number.

Format	`no vlan tagging 1-4093`
Mode	• Interface Config

vlan association subnet

This command associates a VLAN to a specific IP-subnet.

Format	`vlan association subnet ipaddr netmask vlanid`
Mode	VLAN Config

no vlan association subnet

This command removes association of a specific IP-subnet to a VLAN.

Format	`no vlan association subnet` *`ipaddr netmask`*
Mode	VLAN Config

vlan association mac

This command associates a MAC address to a VLAN.

Format	`vlan association mac` *`macaddr vlanid`*
Mode	VLAN database

no vlan association mac

This command removes the association of a MAC address to a VLAN.

Format	`no vlan association mac` *`macaddr`*
Mode	VLAN database

remote-span

This command identifies the VLAN as the RSPAN VLAN.

Default	None
Format	`remote-span`
Mode	VLAN configuration

no remote-span

This command clears RSPAN information for the VLAN.

Format	`no remote-span`
Mode	VLAN configuration

show vlan

This command displays information about the configured private VLANs, including primary and secondary VLAN IDs, type (community, isolated, or primary) and the ports which belong to a private VLAN.

Format	`show vlan {`*`vlanid`*`| private-vlan [type]}`
Mode	• Privileged EXEC • User EXEC

Column	Meaning
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 (Remote Authentication Dial In User Service)*-assigned VLAN does not exist on the switch.
Interface	unit/slot/port. It is possible to set the parameters for all ports by using the selectors on the top line.
Current	The degree of participation of this port in this VLAN. The permissible values are: • Include - This port is always a member of this VLAN. This is equivalent to registration fixed in the IEEE 802.1Q standard. • Exclude - This port is never a member of this VLAN. This is equivalent to registration forbidden in the IEEE 802.1Q standard. • Autodetect - To allow the port to be dynamically registered in this VLAN via GVRP. The port will not participate in this VLAN unless a join request is received on this port. This is equivalent to registration normal in the IEEE 802.1Q standard.
Configured	The configured degree of participation of this port in this VLAN. The permissible values are: • Include - This port is always a member of this VLAN. This is equivalent to registration fixed in the IEEE 802.1Q standard. • Exclude - This port is never a member of this VLAN. This is equivalent to registration forbidden in the IEEE 802.1Q standard. • Autodetect - To allow the port to be dynamically registered in this VLAN via GVRP. The port will not participate in this VLAN unless a join request is received on this port. This is equivalent to registration normal in the IEEE 802.1Q standard.
Tagging	The tagging behavior for this port in this VLAN. • Tagged - Transmit traffic for this VLAN as tagged frames. • Untagged - Transmit traffic for this VLAN as untagged frames.

show vlan internal usage

This command displays information about the VLAN ID allocation on the switch.

Format	`show vlan internal usage`
Mode	• Privileged EXEC • User EXEC

Column	Meaning
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.

show vlan brief

This command displays a list of all configured VLANs.

Format	`show vlan brief`
Mode	• Privileged EXEC • User EXEC

Column	Meaning
VLAN ID	There is a VLAN Identifier (vlanid) associated with each VLAN. The range of the VLAN ID is 1 to 4093.
VLAN Name	A string associated with this VLAN as a convenience. It can be up to 32 alphanumeric characters long, including blanks. The default is blank. VLAN ID 1 always has a name of “Default.” This field is optional.
VLAN Type	Type of VLAN, which can be Default (VLAN ID = 1) or static (one that is configured and permanently defined), or a Dynamic (one that is created by GVRP registration).

show vlan port

This command displays VLAN port information.

Format	`show vlan port {`*`unit/slot/port`*` | all}`
Mode	• Privileged EXEC • User EXEC

Column	Meaning
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 Configured	The VLAN ID that this port will assign to untagged frames or priority tagged frames received on this port. The value must be for an existing VLAN. The factory default is 1.
Port VLAN ID Current	The current VLAN ID that this port assigns to untagged frames or priority tagged frames received on this port. The factory default is 1.
Acceptable Frame Types	The types of frames that may be received on this port. The options are 'VLAN only' and 'Admit All'. When set to 'VLAN only', untagged frames or priority tagged frames received on this port are discarded. When set to 'Admit All', untagged frames or priority tagged frames received on this port are accepted and assigned the value of the Port VLAN ID for this port. With either option, VLAN tagged frames are forwarded in accordance to the 802.1Q VLAN specification.
Ingress Filtering Configured	May be enabled or disabled. When enabled, the frame is discarded if this port is not a member of the VLAN with which this frame is associated. In a tagged frame, the VLAN is identified by the VLAN ID in the tag. In an untagged frame, the VLAN is the Port VLAN ID specified for the port that received this frame. When disabled, all frames are forwarded in accordance with the 802.1Q VLAN bridge specification. The factory default is disabled.
Ingress Filtering Current	Shows the current ingress filtering configuration.

Column	Meaning
GVRP	May be enabled or disabled.
Default Priority	The 802.1p priority assigned to tagged packets arriving on the port.
Protected Port	Specifies if this is a protected port. If False, it is not a protected port; If true, it is.
Switchport mode	The current switchport mode for the port.
Operating parameters	The operating parameters for the port, including the VLAN, name, egress rule, and type.
Static configuration	The static configuration for the port, including the VLAN, name, and egress rule.
Forbidden VLANs	The forbidden VLAN configuration for the port, including the VLAN and name.

show vlan association subnet

This command displays the VLAN associated with a specific configured IP-Address and net mask. If no IP address and net mask are specified, the VLAN associations of all the configured IP-subnets are displayed.

Format	`show vlan association subnet [ipaddr netmask]`
Mode	Privileged EXEC

Column	Meaning
IP Address	The IP address assigned to each interface.
Net Mask	The subnet mask.
VLAN ID	There is a VLAN Identifier (VID) associated with each VLAN.

show vlan association mac

This command displays the VLAN associated with a specific configured MAC address. If no MAC address is specified, the VLAN associations of all the configured MAC addresses are displayed.

Format	`show vlan association mac [macaddr]`
Mode	Privileged EXEC

Column	Meaning
Mac Address	A MAC address for which the switch has forwarding and or filtering information. The format is 6 or 8 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB. In an IVL system the MAC address will be displayed as 8 bytes.
VLAN ID	There is a VLAN Identifier (VID) associated with each VLAN.

Private VLAN Commands

This section describes the commands you use for private VLANs. Private VLANs provides Layer 2 isolation between ports that share the same broadcast domain. In other words, it allows a VLAN broadcast domain to be partitioned into smaller point-to-multipoint subdomains. The ports participating in a private VLAN can be located anywhere in the Layer 2 network.

switchport private-vlan

This command defines a private-VLAN association for an isolated or community port or a mapping for a promiscuous port.

Format	`switchport private-vlan {`**`host-association`** *`primary-vlan-id secondary-vlan-id`* `|` **`mapping`** *`primary-vlan-id`* `{add | remove} secondary-vlan-list}`
Mode	Interface Config

Parameter	Description
`host-association`	Defines the VLAN association for community or host ports.
`mapping`	Defines the private VLAN mapping for promiscuous ports.
`primary-vlan-id`	Primary VLAN ID of a private VLAN.
`secondary-vlan-id`	Secondary (isolated or community) VLAN ID of a private VLAN.
`add`	Associates the secondary VLAN with the primary one.
`remove`	Deletes the secondary VLANs from the primary VLAN association.
`secondary-vlan-list`	A list of secondary VLANs to be mapped to a primary VLAN.

no switchport private-vlan

This command removes the private-VLAN association or mapping from the port.

Format	`no switchport private-vlan {`**`host-association`**`|` **`mapping`**`}`
Mode	Interface Config

switchport mode private-vlan

This command configures a port as a promiscuous or host private VLAN port. Note that the properties of each mode can be configured even when the switch is not in that mode. However, they will only be applicable once the switch is in that particular mode.

Default	general
Format	`switchport mode private-vlan {`**`host`**`|` **`promiscuous`**`}`
Mode	Interface Config

Parameter	Description
host	Configures an interface as a private VLAN host port. It can be either isolated or community port depending on the secondary VLAN it is associated with.
promiscuous	Configures an interface as a private VLAN promiscuous port. The promiscuous ports are members of the primary VLAN.

no switchport mode private-vlan

This command removes the private-VLAN association or mapping from the port.

Format	`no switchport mode private-vlan`
Mode	Interface Config

private-vlan

This command configures the private VLANs and configures the association between the primary private VLAN and secondary VLANs.

Format	`private-vlan {`**`association`** `[add | remove] community|isolated| primary}`
Mode	VLAN Config

Note

This command is available only when you use `vlan` *`vlan_id`* - not `vlan database` - to enter VLAN Config mode.

Parameter	Description
association	Associates the primary and secondary VLAN.
community	Designates a VLAN as a community VLAN.
isolated	Designates a VLAN as the isolated VLAN.
primary	Designates a VLAN as the primary VLAN.

no private-vlan

This command restores normal VLAN configuration.

Format	`no private-vlan {association}`
Mode	VLAN Config

Switch Ports

This section describes the commands used for switch port mode.

switchport mode

Use this command to configure the mode of a switch port as access, trunk or general.

In Trunk mode, the port becomes a member of all VLANs on switch unless specified in the allowed list in the `switchport trunk allowed vlan` command. The PVID of the port is set to the Native VLAN as specified in the `switchport trunk native vlan` command. It means that trunk ports accept both tagged and untagged packets, where untagged packets are processed on the native VLAN and tagged packets are processed on the VLAN ID contained in the packet. MAC learning is performed on both tagged and untagged packets. Tagged packets received with a VLAN ID of which the port is not a member are discarded and MAC learning is not performed. The Trunk ports always transmit packets untagged on native VLAN.

In Access mode, the port becomes a member of only one VLAN. The port sends and receives untagged traffic. It can also receive tagged traffic. The ingress filtering is enabled on port. It means that when the VLAN ID of received packet is not identical to Access VLAN ID, the packet is discarded.

In General mode, the user can perform custom configuration of VLAN membership, PVID, tagging, and ingress filtering.

Default	general
Format	`switchport mode {access | trunk | general}`
Mode	Interface Config

no switchport mode

This command resets the switch port mode to its default value.

Format	`no switchport mode`
Mode	Interface Config

switchport trunk allowed vlan

Use this command to configure the list of allowed VLANs that can receive and send traffic on this interface in tagged format when in trunking mode. The default is all.

The VLANs list can be modified using the add or remove options or replaced with another list using the vlan-list, all, or except options. If all is chosen, all VLANs are added to the list of allowed vlan. The except option provides an exclusion list.

Trunk ports accept tagged packets, where tagged packets are processed on the VLAN ID contained in the packet, if this VLAN is in the allowed VLAN list. Tagged packets received with a VLAN ID to which the port is not a member are discarded and MAC learning is not performed. If a VLAN is added to the system after a port is set to the Trunk mode and it is in the allowed VLAN list, this VLAN is assigned to this port automatically.

Default	all
Format	`switchport trunk allowed vlan {`*`vlan-list`* `| all | {`**`add`** *`vlan-list`*`} | {`**`remove`** *`vlan-list`*`} | {`**`except`** *`vlan-list`* `}}`
Mode	Interface Config

Parameter	Description
all	Specifies all VLANs from 1 to 4093. This keyword is not allowed on commands that do not permit all VLANs in the list to be set at the same time.
add	Adds the defined list of VLANs to those currently set instead of replacing the list.
remove	Removes the defined list of VLANs from those currently set instead of replacing the list. Valid IDs are from 1 to 4093; extended-range VLAN IDs of the form X-Y or X,Y,Z are valid in this command.
except	Lists the VLANs that should be calculated by inverting the defined list of VLANs. (VLANs are added except the ones specified.)
vlan-list	Either a single VLAN number from 1 to 4093 or a continuous range of VLANs described by two VLAN numbers, the lesser one first, separated by a hyphen.

no switchport trunk allowed vlan

This command resets the list of allowed VLANs on the trunk port to its default value.

Format	`no switchport trunk allowed vlan`
Mode	Interface Config

switchport trunk native vlan

Use this command to configure the Trunk port Native VLAN (PVID) parameter. Any ingress untagged packets on the port are tagged with the value of Native VLAN. Native VLAN must be in the allowed VLAN list for tagging of received untagged packets. Otherwise, untagged packets are discarded. Packets marked with Native VLAN are transmitted untagged from Trunk port. The default is 1.

Default	1 (Default VLAN)
Format	`switchport trunk native vlan` *`vlan-id`*
Mode	Interface Config

no switchport trunk native vlan

Use this command to reset the switch port trunk mode native VLAN to its default value.

Format	`no switchport trunk native vlan`
Mode	Interface Config

switchport access vlan

Use this command to configure the VLAN on the Access port. Only one VLAN can be assigned to the Access port. Access ports are members of VLAN 1 by default. Access ports may be assigned to a VLAN other than VLAN 1. Removing the Access VLAN on the switch makes the Access port a member of VLAN 1. Configuring an Access port to be a member of a VLAN that does not exist results in an error and does not change the configuration.

Default	1 (Default VLAN)
Format	`switchport access vlan` *`vlan-id`*
Mode	Interface Config

no switchport access vlan

This command resets the switch port access mode VALN to its default value.

Format	`no switchport access vlan`
Mode	Interface Config

show interfaces switchport

Use this command to display the switchport status for all interfaces or a specified interface.

Format	`show interfaces switchport` *`unit/slot/port`*
Mode	Privileged EXEC

```
(Extreme 220) (Routing) #show interfaces switchport 1/0/1
Port: 1/0/1
VLAN Membership Mode: General
Access Mode VLAN: 1 (default)
General Mode PVID: 1 (default)
General Mode Ingress Filtering: Disabled
General Mode Acceptable Frame Type: Admit all
General Mode Dynamically Added VLANs:
General Mode Untagged VLANs: 1
General Mode Tagged VLANs:
General Mode Forbidden VLANs:
Trunking Mode Native VLAN: 1 (default)
Trunking Mode Native VLAN tagging: Disable
Trunking Mode VLANs Enabled: All
Protected Port: False
 #show interfaces switchport
Port: 1/0/1
VLAN Membership Mode: General
Access Mode VLAN: 1 (default)
General Mode PVID: 1 (default)
General Mode Ingress Filtering: Disabled
General Mode Acceptable Frame Type: Admit all
General Mode Dynamically Added VLANs:
General Mode Untagged VLANs: 1
General Mode Tagged VLANs:
General Mode Forbidden VLANs:
Trunking Mode Native VLAN: 1 (default)
```

```
Trunking Mode Native VLAN tagging: Disable
Trunking Mode VLANs Enabled: All
Protected Port: False
```

show interfaces switchport

Use this command to display the Switchport configuration for a selected mode per interface. If the interface is not specified, the configuration for all interfaces is displayed.

Format	`show interfaces switchport {access | trunk | general} [`*`unit/slot/port`*`]`
Mode	Privileged EXEC

```
(Extreme 220) # show interfaces switchport access 1/0/1
Intf      PVID
--------- ----
1/0/1     1
(Extreme 220) # show interfaces switchport trunk 1/0/6
Intf      PVID  Allowed Vlans List
--------- ----- -------------------
1/0/6     1     All
(Extreme 220) # show interfaces switchport general 1/0/5
Intf      PVID  Ingress     Acceptable  Untagged  Tagged   Forbidden  Dynamic
                Filtering   Frame Type  Vlans     Vlans    Vlans      Vlans
--------- ----- ----------  ----------  --------- -------- ---------- ----------
1/0/5     1     Enabled     Admit All   7         10-50,55  9,100-200 88,96
(Extreme 220) # show interfaces switchport general
Intf      PVID  Ingress     Acceptable  Untagged  Tagged   Forbidden  Dynamic
                Filtering   Frame Type  Vlans     Vlans    Vlans      Vlans
--------- ----- ----------  ----------  --------- -------- ---------- ----------
1/0/1     1     Enabled     Admit All   1,4-7     30-40,55  3,100-200 88,96
1/0/2     1     Disabled    Admit All   1         30-40,55  none      none
..
```

Voice VLAN Commands

This section describes the commands you use for Voice VLAN. Voice VLAN enables switch ports to carry voice traffic with defined priority so as to enable separation of voice and data traffic coming onto the port. The benefits of using Voice VLAN is to ensure that the sound quality of an IP phone could be safeguarded from deteriorating when the data traffic on the port is high.

Also the inherent isolation provided by VLANs ensures that inter-VLAN traffic is under management control and that network- attached clients cannot initiate a direct attack on voice components. *QoS (Quality of Service)*-based on IEEE 802.1P *CoS (Class of Service)* uses classification and scheduling to sent network traffic from the switch in a predictable manner. The system uses the source MAC of the traffic traveling through the port to identify the IP phone data flow.

voice vlan (Global Config)

Use this command to enable the Voice VLAN capability on the switch.

Default	Disabled
Format	`voice vlan`
Mode	Global Config

no voice vlan (Global Config)

Use this command to disable the Voice VLAN capability on the switch.

Format	`no voice vlan`
Mode	Global Config

voice vlan (Interface Config)

Use this command to enable the Voice VLAN capability on the interface or range of interfaces.

Default	Disabled
Format	`voice vlan {`**`vlanid`** *`id`* `|` **`dot1p`** *`priority`* `| none | untagged}`
Mode	Interface Config

You can configure Voice VLAN in one of four different ways:

Parameter	Description
`vlan-id`	Configure the IP phone to forward all voice traffic through the specified VLAN. Valid VLAN ID's are from 1 to 4093 (the max supported by the platform).
`dot1p`	Configure the IP phone to use 802.1p priority tagging for voice traffic and to use the default native VLAN (VLAN 0) to carry all traffic. Valid *`priority`* range is 0 to 7.
`none`	Allow the IP phone to use its own configuration to send untagged voice traffic.
`untagged`	Configure the phone to send untagged voice traffic.

no voice vlan (Interface Config)

Use this command to disable the Voice VLAN capability on the interface.

Format	`no voice vlan`
Mode	Interface Config

voice vlan data priority

Use this command to either trust or untrust the data traffic arriving on the Voice VLAN interface or range of interfaces being configured.

Default	trust
Format	`voice vlan data priority {untrust | trust}`
Mode	Interface Config

show voice vlan

Format	`show voice vlan [interface {`*`unit/slot/port`*` | all}]`
Mode	Privileged EXEC

When the interface parameter is not specified, only the global mode of the Voice VLAN is displayed.

Column	Meaning
Administrative Mode	The Global Voice VLAN mode.

When the interface is specified:

Column	Meaning
Voice VLAN Mode	The admin mode of the Voice VLAN on the interface.
Voice VLAN ID	The Voice VLAN ID
Voice VLAN Priority	The do1p priority for the Voice VLAN on the port.
Voice VLAN Untagged	The tagging option for the Voice VLAN traffic.
Voice VLAN *CoS* Override	The Override option for the voice traffic arriving on the port.
Voice VLAN Status	The operational status of Voice VLAN on the port.

Provisioning (IEEE 802.1p) Commands

This section describes the commands used to configure provisioning (IEEE 802.1p,) which allows you to prioritize ports.

vlan port priority all

This command configures the port priority assigned for untagged packets for all ports presently plugged into the device. The range for the priority is 0-7. Any subsequent per port configuration will override this configuration setting.

Format	`vlan port priority all` *`priority`*
Mode	Global Config

vlan priority

This command configures the default 802.1p port priority assigned for untagged packets for a specific interface. The range for the priority is 0–7.

Default	0
Format	`vlan priority` *priority*
Mode	Interface Config

Asymmetric Flow Control

Note
Asymmetric Flow Control can only be configured globally for all ports on XGS4 silicon-based switches.

Note
Asymmetric Flow Control is not supported on Fast Ethernet platforms.

Note
If Asymmetric Flow Control is not supported on the platform, then only symmetric, or no flow control, modes are configurable.

When in asymmetric flow control mode, the switch responds to PAUSE frames received from a peer by stopping packet transmission, but the switch does not initiate MAC control PAUSE frames.

When you configure the switch in asymmetric flow control (or no flow control mode), the device is placed in egress drop mode. Egress drop mode maximizes the throughput of the system at the expense of packet loss in a heavily congested system, and this mode avoids head-of-line blocking.

flowcontrol {symmetric|asymmetric}

Note
The flowcontrol {symmetric|asymmetric} command is available if the platform supports the asymmetric flow control feature.

Use this command to enable or disable the symmetric or asymmetric flow control on the switch. Asymmetric here means that Tx Pause can never be enabled. Only Rx Pause can be enabled.

Default	Flow control is disabled.
Format	`flowcontrol {symmetric|asymmetric}`
Mode	Global Config

no flowcontrol {symmetric|asymmetric}

Use the no form of this command to disable symmetric or asymmetric flow control.

Format	`no flowcontrol {symmetric|asymmetric}`
Mode	Global Config

flowcontrol

Note
This flowcontrol command is available if the platform supports only the symmetric flow control feature.

Use this command to enable or disable the symmetric flow control on the switch.

Default	Flow control is disabled.
Format	`flowcontrol`
Mode	Global Config

no flowcontrol

Use the no form of this command to disable the symmetric flow control.

Format	`no flowcontrol`
Mode	Global Config

show flowcontrol

Use this command to display the IEEE 802.3 Annex 31B flow control settings and status for a specific interface or all interfaces. The command also displays 802.3 Tx and Rx pause counts. Priority Flow Control frames counts are not displayed. If the port is enabled for priority flow control, operational flow control status is displayed as Inactive. Operational flow control status for stacking ports is always displayed as N/A.

Format	`show flowcontrol [`*`unit/slot/port`*`]`
Mode	Privileged EXEC

The following example shows CLI display output for the command.

```
(Extreme 220)#show flowcontrol
Admin Flow Control: Symmetric
Port     Flow Control     RxPause     TxPause
         Oper
------   ------------     --------    ---------
0/1      Active           310         611
0/2      Inactive         0            0
```

The following example shows CLI display output for the command.

```
(Extreme 220)#show flowcontrol interface 0/1
Admin Flow Control: Symmetric
Port        Flow Control  RxPause       TxPause
            Oper
---------   -------       --------      -------
0/1         Active        310           611
```

Protected Ports Commands

This section describes commands used 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 *LAG*, the protected port status becomes operationally disabled on the interface, and the interface follows the configuration of the LAG port. However, the protected port configuration for the interface remains unchanged. Once the interface is no longer a member of a LAG, the current configuration for that interface automatically becomes effective.

switchport protected (Global Config)

Use this command to create a protected port group. The groupid parameter identifies the set of protected ports. Use the name name pair to assign a name to the protected port group. The name can be up to 32 alphanumeric characters long, including blanks. The default is blank.

Note

Port protection occurs within a single switch. Protected port configuration does not affect traffic between ports on two different switches. No traffic forwarding is possible between two protected ports.

Default	Unprotected
Format	`switchport protected` *`groupid`* `name` *`name`*
Mode	Global Config

no switchport protected (Global Config)

Use this command to remove a protected port group. The groupid parameter identifies the set of protected ports. The name keyword specifies the name to remove from the group.

Format	`no switchport protected` *`groupid`* `name`
Mode	Global Config

switchport protected (Interface Config)

Use this command to add an interface to a protected port group. The groupid parameter identifies the set of protected ports to which this interface is assigned. You can only configure an interface as protected in one group.

Note

Port protection occurs within a single switch. Protected port configuration does not affect traffic between ports on two different switches. No traffic forwarding is possible between two protected ports.

Default	Unprotected
Format	`switchport protected groupid`
Mode	Interface Config

no switchport protected (Interface Config)

Use this command to configure a port as unprotected. The groupid parameter identifies the set of protected ports to which this interface is assigned.

Format	`no switchport protected groupid`
Mode	Interface Config

show switchport protected

This command displays the status of all the interfaces, including protected and unprotected interfaces.

Format	`show switchport protected groupid`
Mode	• Privileged EXEC • User EXEC

Column	Meaning
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.

show interfaces switchport

This command displays the status of the interface (protected/unprotected) under the groupid.

Format	`show interfaces switchport unit/slot/port groupid`
Mode	• Privileged EXEC • User EXEC

Column	Meaning
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	Whether the interface is protected or not. It shows TRUE or FALSE. If the group is a multiple groups then it shows TRUE in Group *groupid.*

GARP Commands

This section describes the commands used to configure Generic Attribute Registration Protocol (GARP) and view GARP status. The commands in this section affect both GARP VLAN Registration Protocol (GVRP) and GARP Multicast Registration Protocol (GMRP). GARP is a protocol that allows client stations to register with the switch for membership in VLANS (by using GVMP) or multicast groups (by using GVMP).

set garp timer join

This command sets the GVRP join time per GARP for one interface, a range of interfaces, or all interfaces. Join time is the interval between the transmission of GARP Protocol Data Units (PDUs) registering (or reregistering) membership for a VLAN or multicast group. This command has an effect only when GVRP is enabled. The time is from 10 to 100 (centiseconds). The value 20 centiseconds is 0.2 seconds.

Default	20
Format	`set garp timer join` *`10-100`*
Mode	• Interface Config • Global Config

no set garp timer join

This command sets the GVRP join time to the default and only has an effect when GVRP is enabled.

Format	`no set garp timer join`
Mode	• Interface Config • Global Config

set garp timer leave

This command sets the GVRP leave time for one interface, a range of interfaces, or all interfaces or all ports and only has an effect when GVRP is enabled. Leave time is the time to wait after receiving an unregister request for a VLAN or a multicast group before deleting the VLAN entry. This can be considered a buffer time for another station to assert registration for the same attribute in order to maintain uninterrupted service. The leave time is 20 to 600 (centiseconds). The value 60 centiseconds is 0.6 seconds. The leave time must be greater than or equal to three times the join time.

Default	60
Format	`set garp timer leave` *`20-600`*
Mode	• Interface Config • Global Config

no set garp timer leave

This command sets the GVRP leave time on all ports or a single port to the default and only has an effect when GVRP is enabled.

Format	`no set garp timer leave`
Mode	• Interface Config • Global Config

set garp timer leaveall

This command sets how frequently Leave All PDUs are generated. A Leave All PDU indicates that all registrations will be unregistered. Participants would need to rejoin in order to maintain registration. The value applies per port and per GARP participation. The time may range from 200 to 6000 (centiseconds). The value 1000 centiseconds is 10 seconds. You can use this command on all ports (Global Config mode), or on a single port or a range of ports (Interface Config mode) and it only has an effect only when GVRP is enabled. The leave all time must be greater than the leave time.

Default	1000
Format	`set garp timer leaveall` *`200-6000`*
Mode	• Interface Config • Global Config

no set garp timer leaveall

This command sets how frequently Leave All PDUs are generated the default and only has an effect when GVRP is enabled.

Format	`no set garp timer leaveall`
Mode	• Interface Config • Global Config

show garp

This command displays GARP information.

Format	`show garp`
Mode	• Privileged EXEC • User EXEC

Column	Meaning
GMRP Admin Mode	The administrative mode of GARP Multicast Registration Protocol (GMRP) for the system.
GVRP Admin Mode	The administrative mode of GARP VLAN Registration Protocol (GVRP) for the system.

GVRP Commands

This section describes the commands used to configure and view GARP VLAN Registration Protocol (GVRP) information. GVRP-enabled switches exchange VLAN configuration information, which allows GVRP to provide dynamic VLAN creation on trunk ports and automatic VLAN pruning.

Note
If GVRP is disabled, the system does not forward GVRP messages.

set gvrp adminmode

This command enables GVRP on the system.

Default	Disabled
Format	`set gvrp adminmode`
Mode	Privileged EXEC

no set gvrp adminmode

This command disables GVRP.

Format	`no set gvrp adminmode`
Mode	Privileged EXEC

set gvrp interfacemode

This command enables GVRP on a single port (Interface Config mode), a range of ports (Interface Range mode), or all ports (Global Config mode).

Default	Disabled
Format	`set gvrp interfacemode`
Mode	• Interface Config • Interface Range • Global Config

no set gvrp interfacemode

This command disables GVRP on a single port (Interface Config mode) or all ports (Global Config mode). If GVRP is disabled, Join Time, Leave Time and Leave All Time have no effect.

Format	`no set gvrp interfacemode`
Mode	• Interface Config • Global Config

show gvrp configuration

This command displays Generic Attributes Registration Protocol (GARP) information for one or all interfaces.

Format	`show gvrp configuration {unit/slot/port | all}`
Mode	• Privileged EXEC • User EXEC

Column	Meaning
Interface	*unit/slot/port*
Join Timer	The interval between the transmission of GARP PDUs registering (or reregistering) membership for an attribute. Current attributes are a VLAN or multicast group. There is an instance of this timer on a per-Port, per-GARP participant basis. Permissible values are 10 to 100 centiseconds (0.1 to 1.0 seconds). The factory default is 20 centiseconds (0.2 seconds). The finest granularity of specification is one centisecond (0.01 seconds).
Leave Timer	The period of time to wait after receiving an unregister request for an attribute before deleting the attribute. Current attributes are a VLAN or multicast group. This may be considered a buffer time for another station to assert registration for the same attribute in order to maintain uninterrupted service. There is an instance of this timer on a per-Port, per-GARP participant basis. Permissible values are 20 to 600 centiseconds (0.2 to 6.0 seconds). The factory default is 60 centiseconds (0.6 seconds).
LeaveAll Timer	This Leave All Time controls how frequently LeaveAll PDUs are generated. A LeaveAll PDU indicates that all registrations will shortly be deregistered. Participants will need to rejoin in order to maintain registration. There is an instance of this timer on a per-Port, per-GARP participant basis. The Leave All Period Timer is set to a random value in the range of LeaveAllTime to 1.5*LeaveAllTime. Permissible values are 200 to 6000 centiseconds (2 to 60 seconds). The factory default is 1000 centiseconds (10 seconds).
Port GMRP Mode	The GMRP administrative mode for the port, which is enabled or disabled (default). If this parameter is disabled, Join Time, Leave Time and Leave All Time have no effect.

GMRP Commands

This section describes the commands used to configure and view GARP Multicast Registration Protocol (GMRP) information. Like *IGMP (Internet Group Management Protocol)* snooping, GMRP helps control the flooding of multicast packets. GMRP-enabled switches dynamically register and de-register group membership information with the MAC networking devices attached to the same segment. GMRP also allows group membership information to propagate across all networking devices in the bridged LAN that support Extended Filtering Services.

Note
If GMRP is disabled, the system does not forward GMRP messages.

set gmrp adminmode

This command enables GARP Multicast Registration Protocol (GMRP) on the system.

Default	Disabled
Format	`set gmrp adminmode`
Mode	Privileged EXEC

no set gmrp adminmode

This command disables GARP Multicast Registration Protocol (GMRP) on the system.

Format	`no set gmrp adminmode`
Mode	Privileged EXEC

set gmrp interfacemode

This command enables GARP Multicast Registration Protocol on a single interface (Interface Config mode), a range of interfaces, or all interfaces (Global Config mode). If an interface which has GARP enabled is enabled for routing or is enlisted as a member of a port-channel (*LAG*), GARP functionality is disabled on that interface. GARP functionality is subsequently re-enabled if routing is disabled and port-channel (LAG) membership is removed from an interface that has GARP enabled.

Default	Disabled
Format	`set gmrp interfacemode`
Mode	• Interface Config • Global Config

no set gmrp interfacemode

This command disables GARP Multicast Registration Protocol on a single interface or all interfaces. If an interface which has GARP enabled is enabled for routing or is enlisted as a member of a port-channel (*LAG*), GARP functionality is disabled. GARP functionality is subsequently re-enabled if routing is disabled and port-channel (LAG) membership is removed from an interface that has GARP enabled.

Format	`no set gmrp interfacemode`
Mode	• Interface Config • Global Config

show gmrp configuration

This command displays Generic Attributes Registration Protocol (GARP) information for one or all interfaces.

Format	`show gmrp configuration {`*`unit/slot/port`*` | all}`
Mode	• Privileged EXEC • User EXEC

Column	Meaning
Interface	The *unit/slot/port* of the interface that this row in the table describes.
Join Timer	The interval between the transmission of GARP PDUs registering (or reregistering) membership for an attribute. Current attributes are a VLAN or multicast group. There is an instance of this timer on a per-port, per-GARP participant basis. Permissible values are 10 to 100 centiseconds (0.1 to 1.0 seconds). The factory default is 20 centiseconds (0.2 seconds). The finest granularity of specification is 1 centisecond (0.01 seconds).
Leave Timer	The period of time to wait after receiving an unregister request for an attribute before deleting the attribute. Current attributes are a VLAN or multicast group. This may be considered a buffer time for another station to assert registration for the same attribute in order to maintain uninterrupted service. There is an instance of this timer on a per-Port, per-GARP participant basis. Permissible values are 20 to 600 centiseconds (0.2 to 6.0 seconds). The factory default is 60 centiseconds (0.6 seconds).
LeaveAll Timer	This Leave All Time controls how frequently LeaveAll PDUs are generated. A LeaveAll PDU indicates that all registrations will shortly be deregistered. Participants will need to rejoin in order to maintain registration. There is an instance of this timer on a per-Port, per-GARP participant basis. The Leave All Period Timer is set to a random value in the range of LeaveAllTime to 1.5*LeaveAllTime. Permissible values are 200 to 6000 centiseconds (2 to 60 seconds). The factory default is 1000 centiseconds (10 seconds).
Port GMRP Mode	The GMRP administrative mode for the port. It may be enabled or disabled. If this parameter is disabled, Join Time, Leave Time and Leave All Time have no effect.

show mac-address-table gmrp

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

Format	`show mac-address-table gmrp`
Mode	Privileged EXEC

Column	Meaning
VLAN ID	The VLAN in which the MAC Address is learned.
MAC Address	A unicast MAC address for which the switch has forwarding and or filtering information. The format is 6 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB.
Type	The type of the entry. Static entries are those that are configured by the end user. Dynamic entries are added to the table as a result of a learning process or protocol.
Description	The text description of this multicast table entry.
Interfaces	The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).

Port-Based Network Access Control Commands

This section describes the commands used to configure port-based network access control (IEEE 802.1X). Port-based network access control allows you to permit access to network services only to and devices that are authorized and authenticated.

aaa authentication dot1x default

Use this command to configure the authentication method for port-based access to the switch. The additional methods of authentication are used only if the previous method returns an error, not if there is an authentication failure. The possible methods are as follows:

- ias. Uses the internal authentication server users database for authentication. This method can be used in conjunction with any one of the existing methods like local or RADIUS.
- local. Uses the local username database for authentication.
- none. Uses no authentication.
- radius. Uses the list of all *RADIUS* servers for authentication.

Format	`aaa authentication dot1x default {[ias]|[`*`method1 [method2 [method3]]]`*`}`
Mode	Global Config

The following is an example of the command.

```
(Extreme 220) #configure
(Extreme 220) (Config) #aaa authentication dot1x default ias none
(Extreme 220) (Config) #aaa authentication dot1x default ias local radius none
```

clear dot1x statistics

This command resets the 802.1X statistics for the specified port or for all ports.

Format	`clear dot1x statistics {`*`unit/slot/port`*` | all}`
Mode	Privileged EXEC

clear dot1x authentication-history

This command clears the authentication history table captured during successful and unsuccessful authentication on all interface or the specified interface.

Format	`clear dot1x authentication-history [`*`unit/slot/port`*`]`
Mode	Privileged EXEC

clear radius statistics

This command is used to clear all *RADIUS* statistics.

Format	`clear radius statistics`
Mode	Privileged EXEC

dot1x eapolflood

Use this command to enable EAPOL flood support on the switch.

Default	disabled
Format	`dot1x eapolflood`
Mode	Global Config

no dot1x eapolflood

This command disables EAPOL flooding on the switch.

Format	`no dot1x eapolflood`
Mode	Global Config

dot1x dynamic-vlan enable

Use this command to enable the switch to create VLANs dynamically when a *RADIUS*-assigned VLAN does not exist in the switch.

Default	Disabled
Format	`dot1x dynamic-vlan enable`
Mode	Global Config

no dot1x dynamic-vlan enable

Use this command to prevent the switch from creating VLANs when a *RADIUS*-assigned VLAN does not exist in the switch.

Format	`no dot1x dynamic-vlan enable`
Mode	Global Config

dot1x port-control

This command sets the authentication mode to use on the specified interface or range of interfaces. Use the force-unauthorized parameter to specify that the authenticator PAE unconditionally sets the controlled port to unauthorized. Use the force-authorized parameter to specify that the authenticator PAE unconditionally sets the controlled port to authorized. Use the auto parameter to specify that the authenticator PAE sets the controlled port mode to reflect the outcome of the authentication exchanges between the supplicant, authenticator and the authentication server. If the mac-based option is specified, then MAC-based dot1x authentication is enabled on the port.

Default	auto
Format	`dot1x port-control {force-unauthorized | force-authorized | auto | mac-based}`
Mode	Interface Config

no dot1x port-control

This command sets the 802.1X port control mode on the specified port to the default value.

Format	`no dot1x port-control`
Mode	Interface Config

dot1x port-control all

This command sets the authentication mode to use on all ports. Select force-unauthorized to specify that the authenticator PAE unconditionally sets the controlled port to unauthorized. Select force-authorized to specify that the authenticator PAE unconditionally sets the controlled port to authorized. Select auto to specify that the authenticator PAE sets the controlled port mode to reflect the outcome of the authentication exchanges between the supplicant, authenticator and the authentication server. If the mac-based option is specified, then MAC-based dot1x authentication is enabled on the port.

Default	auto
Format	`dot1x port-control all {force-unauthorized | force-authorized | auto | mac-based}`
Mode	Global Config

no dot1x port-control all

This command sets the authentication mode on all ports to the default value.

Format	`no dot1x port-control all`
Mode	Global Config

dot1x system-auth-control

Use this command to enable the dot1x authentication support on the switch. While disabled, the dot1x configuration is retained and can be changed, but is not activated.

Default	disabled
Format	`dot1x system-auth-control`
Mode	Global Config

no dot1x system-auth-control

This command is used to disable the dot1x authentication support on the switch.

Format	`no dot1x system-auth-control`
Mode	Global Config

dot1x system-auth-control monitor

Use this command to enable the 802.1X monitor mode on the switch. The purpose of Monitor mode is to help troubleshoot port-based authentication configuration issues without disrupting network access for hosts connected to the switch. In Monitor mode, a host is granted network access to an 802.1X-enabled port even if it fails the authentication process. The results of the process are logged for diagnostic purposes.

Default	disabled
Format	`dot1x system-auth-control monitor`
Mode	Global Config

no dot1x system-auth-control monitor

This command disables the 802.1X Monitor mode on the switch.

Format	`no dot1x system-auth-control monitor`
Mode	Global Config

dot1x user

This command adds the specified user to the list of users with access to the specified port or all ports. The user parameter must be a configured user.

Format	`dot1x user` *`user`* `{`*`unit/slot/port`* `| all}`
Mode	Global Config

no dot1x user

This command removes the user from the list of users with access to the specified port or all ports.

Format	`no dot1x user` *`user`* `{`*`unit/slot/port`* `| all}`
Mode	Global Config

authentication enable

This command globally enables the Authentication Manager. Interface configuration takes effect only if the Authentication Manager is enabled with this command.

Default	disabled
Format	*authentication enable*
Mode	Global Config

no authentication enable

This command disables the Authentication Manager.

Format	*no authentication enable*
Mode	Global Config

authentication order

This command sets the order of authentication methods used on a port. The available authentication methods are Dot1x, MAB, and captive portal. Ordering sets the order of methods that the switch attempts when trying to authenticate a new device connected to a port. If one method is unsuccessful or timed out, the next method is attempted.

Each method can only be entered once. Ordering is only possible between 802.1x and MAB.

Note
Captive portal is not supported in this version of the product.

Format	`authentication order {dot1x [mab [captive-portal] | captive-portal] | mab [dot1x [captive-portal]| captive-portal] | captive-portal}`
Mode	Interface Config

no authentication order

This command returns the port to the default authentication order.

Format	*no authentication order*
Mode	Interface Config

authentication priority

This command sets the priority for the authentication methods used on a port. The available authentication methods are Dot1x, MAB, and captive portal. The authentication priority decides if a

previously authenticated client is reauthenticated with a higher-priority method when the same is received.

Note
Captive portal is always the last method in the list. It is not supported in this version of the product.

Default	authentication order dot1x mab captive portal
Format	`authentication priority {dot1x [mab [captive portal] | captive portal] | mab [dot1x [captive portal]| captive portal] | captive portal}`
Mode	Interface Config

no authentication priority

This command returns the port to the default order of priority for the authentication methods.

Format	*`no authentication priority`*
Mode	Interface Config

authentication timer restart

This command sets the time, in seconds, after which reauthentication starts. (The default time is 300 seconds.) The timer restarts the authentication only after all the authentication methods fail. At the expiration of this timer, authentication is reinitiated for the port.

Format	*`authentication timer restart 300-65535`*
Mode	Interface Config

no authentication timer restart

This command sets the reauthentication value to the default value of 3600 seconds.

Format	*`no authentication timer restart`*
Mode	Interface Config

show authentication authentication-history

Use this command to display information about the authentication history for a specified interface.

Format	`show authentication authentication-history` *`unit/slot/port`*
Mode	Privileged EXEC

Term	Definition
Time Stamp	The time of the authentication.
Interface	The interface.
MAC-Address	The MAC address for the interface.
Auth Status Method	The authentication method and status for the interface.

The following information is shown for the interface.

```
Time Stamp            Interface MAC-Address     Auth Status  Method
--------------------- --------- ----------------- ------ ------------
Jul 21 1919 15:06:15  1/0/1     00:00:00:00:00:01 Authorized  802.1X
```

show authentication interface

Use this command to display authentication method information either for all interfaces or a specified port.

Format	`show authentication interface {all | unit/slot/port }`
Mode	Privileged EXEC

The following information is displayed for each interface.

Term	Definition
Interface	The interface for which authentication configuration information is being displayed.
Authentication Restart timer	The time, in seconds, after which reauthentication starts.
Configured method order	The order of authentication methods used on a port.
Enabled method order	The order of authentication methods used on a port.
Configured method priority	The priority for the authentication methods used on a port.
Enabled method priority	The priority for the authentication methods used on a port.
Number of authenticated clients	The number of authenticated clients.
Logical Interface	The logical interface
Client MAC addr	The MAC address for the client.
Authenticated Method	The current authentication method.
Auth State	If the authentication was successful.

Term	Definition
Auth Status	The current authentication status.

The following example displays the authentication interface information for all interfaces.

Note
Although `captive-portal` is displayed in the command output, captive portal is not supported in this version of the product.

```
(Extreme 220) #show authentication interface all
Interface..................................... 1/0/1
Authentication Restart timer.................. 300
Configured method order....................... dot1x mab captive-portal
Enabled method order.......................... dot1x mab undefined
Configured method priority.................... undefined undefined undefined
Enabled method priority....................... undefined undefined undefined
Number of authenticated clients............... 0
Interface..................................... 1/0/2
Authentication Restart timer.................. 300
Configured method order....................... dot1x mab captive-portal
Enabled method order.......................... dot1x mab undefined
Configured method priority.................... undefined undefined undefined
Enabled method priority....................... undefined undefined undefined
Number of authenticated clients............... 0
Interface..................................... 1/0/3
Authentication Restart timer.................. 300
Configured method order....................... dot1x mab captive-portal
Enabled method order.......................... dot1x mab undefined
Configured method priority.................... undefined undefined undefined
Enabled method priority....................... undefined undefined undefined
Number of authenticated clients............... 0
Interface..................................... 1/0/4
Authentication Restart timer.................. 300
Configured method order....................... dot1x mab captive-portal
Enabled method order.......................... dot1x mab undefined
Configured method priority.................... undefined undefined undefined
Enabled method priority....................... undefined undefined undefined
Number of authenticated clients............... 0
```

show authentication methods

Use this command to display information about the authentication methods.

Format	`show authentication methods`
Mode	Privileged EXEC

Term	Definition
Authentication Login List	The authentication login listname.
Method 1	The first method in the specified authentication login list, if any.
Method 2	The second method in the specified authentication login list, if any.

Term	Definition
Method 3	The third method in the specified authentication login list, if any.

The following example displays the authentication configuration.

```
(Extreme 220) #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
HTTPS       :local
HTTP        :local
DOT1X       :
```

show authentication statistics

Use this command to display the authentication statistics for an interface.

Format	*show authentication statistics unit/slot/port*
Mode	Privileged EXEC

The following information is displayed for each interface.

Term	Definition
Port	The port for which information is being displayed.
802.1X attempts	The number of Dot1x authentication attempts for the port.
802.1X failed attempts	The number of failed Dot1x authentication attempts for the port.
Mab attempts	The number of MAB (MAC authentication bypass) authentication attempts for the port.
Mab failed attempts	The number of failed MAB authentication attempts for the port.
Captive-portal attempts	The number of captive portal (web authorization) authentication attempts for the port.

Note
Captive portal is not supported in this version of the product.

Term	Definition
Captive-portal failed attempts	The number of failed captive portal authentication attempts for the port.

Note
Captive portal is not supported in this version of the product.

```
(Extreme 220) (Routing) #show authentication statistics 1/0/1
Port..................................... 1/0/1
802.1X attempts.......................... 0
802.1X failed attempts................... 0
Mab attempts............................. 0
Mab failed attempts...................... 0
Captive-portal attempts.................. 0
Captive-Portal failed attempts........... 0
```

clear authentication statistics

Use this command to clear the authentication statistics on an interface.

Format	*clear authentication authentication-history {unit/slot/port] | all}*
Mode	Privileged EXEC

clear authentication authentication-history

Use this command to clear the authentication history log for an interface.

Format	*clear authentication authentication-history {unit/slot/port | all}*
Mode	Privileged EXEC

show dot1x

This command is used to show a summary of the global dot1x configuration, summary information of the dot1x configuration for a specified port or all ports, the detailed dot1x configuration for a specified port and the dot1x statistics for a specified port – depending on the tokens used.

Format	show dot1x [{*summary* {*unit/slot/port* | all} | detail *unit/slot/port* | statistics *unit/slot/port*]
Mode	Privileged EXEC

If you do not use the optional parameters unit/slot/port or vlanid, the command displays the global dot1x mode, the VLAN Assignment mode, and the Dynamic VLAN Creation mode.

Term	Definition
Administrative Mode	Whether authentication control on the switch is enabled or disabled.
VLAN Assignment Mode	Whether assignment of an authorized port to a *RADIUS*-assigned VLAN is allowed (enabled) or not (disabled).
Dynamic VLAN Creation Mode	Whether the switch can dynamically create a RADIUS-assigned VLAN if it does not currently exist on the switch.
Monitor Mode	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.

Term	Definition
Interface	The interface whose configuration is displayed.
Control Mode	The configured control mode for this port. Possible values are force-unauthorized | force-authorized | auto | mac-based | authorized | unauthorized.
Operating Control Mode	The control mode under which this port is operating. Possible values are authorized | unauthorized.
Reauthentication Enabled	Whether reauthentication is enabled on this port.
Port Status	Whether the port is authorized or unauthorized. Possible values are authorized | unauthorized.

The following example shows CLI display output for the command `show dot1x summary 0/1`.

```
                                    Operating
Interface        Control Mode       Control Mode         Port Status
---------        ------------       ------------         ------------
0/1              auto               auto                 Authorized
```

If you use the optional parameter 'detail unit/slot/port', the detailed dot1x configuration for the specified port is displayed.

Term	Definition
Port	The interface whose configuration is displayed.
Protocol Version	The protocol version associated with this port. The only possible value is 1, corresponding to the first version of the dot1x specification.
PAE Capabilities	The port access entity (PAE) functionality of this port. Possible values are Authenticator or Supplicant.
Control Mode	The configured control mode for this port. Possible values are force-unauthorized | force-authorized | auto | mac-based.
Authenticator PAE State	Current state of the authenticator PAE state machine. Possible values are Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, ForceAuthorized, and ForceUnauthorized. When MAC-based authentication is enabled on the port, this parameter is deprecated.
Backend Authentication State	Current state of the backend authentication state machine. Possible values are Request, Response, Success, Fail, Timeout, Idle, and Initialize. When MAC-based authentication is enabled on the port, this parameter is deprecated.
Quiet Period	The timer used by the authenticator state machine on this port to define periods of time in which it will not attempt to acquire a supplicant. The value is expressed in seconds and will be in the range 0 and 65535.

Term	Definition
Transmit Period	The timer used by the authenticator state machine on the specified port to determine when to send an EAPOL EAP Request/Identity frame to the supplicant. The value is expressed in seconds and will be in the range of 1 and 65535.
Guest-VLAN ID	The guest VLAN identifier configured on the interface.
Guest VLAN Period	The time in seconds for which the authenticator waits before authorizing and placing the port in the Guest VLAN, if no EAPOL packets are detected on that port.
Supplicant Timeout	The timer used by the authenticator state machine on this port to timeout the supplicant. The value is expressed in seconds and will be in the range of 1 and 65535.
Server Timeout	The timer used by the authenticator on this port to timeout the authentication server. The value is expressed in seconds and will be in the range of 1 and 65535.
Maximum Requests	The maximum number of times the authenticator state machine on this port will retransmit an EAPOL EAP Request/Identity before timing out the supplicant. The value will be in the range of 1 and 10.
Configured MAB Mode	The administrative mode of the MAC authentication bypass feature on the switch.
Operational MAB Mode	The operational mode of the MAC authentication bypass feature on the switch. MAB might be administratively enabled but not operational if the control mode is not MAC based.
Vlan-ID	The VLAN assigned to the port by the RADIUS server. This is only valid when the port control mode is not MAC-based.
VLAN Assigned Reason	The reason the VLAN identified in the VLAN-assigned field has been assigned to the port. Possible values are RADIUS, Unauthenticated VLAN, Guest VLAN, default, and Not Assigned. When the VLAN Assigned Reason is Not Assigned, it means that the port has not been assigned to any VLAN by dot1x. This only valid when the port control mode is not MAC-based.
Reauthentication Period	The timer used by the authenticator state machine on this port to determine when reauthentication of the supplicant takes place. The value is expressed in seconds and will be in the range of 1 and 65535.
Reauthentication Enabled	Whether reauthentication is enabled on this port. Possible values are ‘True” or “False”.
Key Transmission Enabled	Whether the key is transmitted to the supplicant for the specified port. Possible values are True or False.
EAPOL Flood Mode Enabled	Whether the EAPOL flood support is enabled on the switch. Possible values are True or False.
Control Direction	The control direction for the specified port or ports. Possible values are both or in.
Maximum Users	The maximum number of clients that can get authenticated on the port in the MAC-based dot1x authentication mode. This value is used only when the port control mode is not MAC-based.
Unauthenticated VLAN ID	The unauthenticated VLAN configured for this port. This value is valid for the port only when the port control mode is not MAC-based.
Session Timeout	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 the port goes into unauthorized state. If the value is **`Radius-Request`**,

Term	Definition
	then a reauthentication of the client authenticated on the port is performed. This value is valid for the port only when the port control mode is not MAC-based.

The following example shows CLI display output for the command.

```
(Extreme 220) #show dot1x detail 1/0/3
Port..................................... 1/0/1
Protocol Version......................... 1
PAE Capabilities......................... Authenticator
Control Mode............................. auto
Authenticator PAE State.................. Initialize
Backend Authentication State............. Initialize
Quiet Period (secs)...................... 60
Transmit Period (secs)................... 30
Guest VLAN ID............................ 0
Guest VLAN Period (secs)................. 90
Supplicant Timeout (secs)................ 30
Server Timeout (secs).................... 30
Maximum Requests......................... 2
Configured MAB Mode...................... Enabled
Operational MAB Mode..................... Disabled
VLAN Id.................................. 0
VLAN Assigned Reason..................... Not Assigned
Reauthentication Period (secs)........... 3600
Reauthentication Enabled................. FALSE
Key Transmission Enabled................. FALSE
EAPOL flood Mode Enabled................. FALSE
Control Direction........................ both
Maximum Users............................ 16
Unauthenticated VLAN ID.................. 0
Session Timeout.......................... 0
Session Termination Action............... Default
```

For each client authenticated on the port, the show dot1x detail unit/slot/port command will display the following MAC-based dot1x parameters if the port-control mode for that specific port is MAC-based.

Term	Definition
Supplicant MAC-Address	The MAC-address of the supplicant.
Authenticator PAE State	Current state of the authenticator PAE state machine. Possible values are Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, ForceAuthorized, and ForceUnauthorized.
Backend Authentication State	Current state of the backend authentication state machine. Possible values are Request, Response, Success, Fail, Timeout, Idle, and Initialize.
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.

Term	Definition
Port	The interface whose statistics are displayed.
EAPOL Frames Received	The number of valid EAPOL frames of any type that have been received by this authenticator.

Term	Definition
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.
Invalid EAPOL Frames Received	The number of EAPOL frames that have been received by this authenticator in which the frame type is not recognized.
EAP Length Error Frames Received	The number of EAPOL frames that have been received by this authenticator in which the frame type is not recognized.

show dot1x authentication-history

This command displays 802.1X authentication events and information during successful and unsuccessful Dot1x authentication process for all interfaces or the specified interface. Use the optional keywords to display only failure authentication events in summary or in detail.

Format	`show dot1x authentication-history {`*`unit/slot/port`* `| all} [failed-auth-only] [detail]`
Mode	Privileged EXEC

Term	Definition
Time Stamp	The exact time at which the event occurs.
Interface	Physical Port on which the event occurs.
Mac-Address	The supplicant/client MAC address.
VLAN assigned	The VLAN assigned to the client/port on authentication.
VLAN assigned Reason	The type of VLAN ID assigned, which can be Guest VLAN, Unauth, Default, *RADIUS* Assigned, or Monitor Mode VLAN ID.
Auth Status	The authentication status.
Reason	The actual reason behind the successful or failed authentication.

show dot1x clients

This command displays 802.1X client information. This command also displays information about the number of clients that are authenticated using Monitor mode and using 802.1X.

Format	`show dot1x clients {unit/slot/port | all}`
Mode	Privileged EXEC

Term	Definition
Clients Authenticated using Monitor Mode	The number of the Dot1x clients authenticated using Monitor mode.
Clients Authenticated using Dot1x	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.

show dot1x users

This command displays 802.1X port security user information for locally configured users.

Format	`show dot1x users unit/slot/port`
Mode	Privileged EXEC

Term	Definition
Users	Users configured locally to have access to the specified port.

802.1X Supplicant Commands

200 Series supports 802.1X ("dot1x") supplicant functionality on point-to-point ports. The administrator can configure the user name and password used in authentication and capabilities of the supplicant port.

dot1x pae

This command sets the port's dot1x role. The port can serve as either a supplicant or an authenticator.

Format	`dot1x pae {supplicant | authenticator}`
Mode	Interface Config

dot1x supplicant port-control

This command sets the ports authorization state (Authorized or Unauthorized) either manually or by setting the port to auto-authorize upon startup. By default all the ports are authenticators. If the port's attribute needs to be moved from <authenticator to supplicant> or <supplicant to authenticator>, use this command.

Format	`dot1x supplicant port-control {auto | force-authorized | force_unauthorized}`
Mode	Interface Config

Parameter	Description
auto	The port is in the Unauthorized state until it presents its user name and password credentials to an authenticator. If the authenticator authorizes the port, then it is placed in the Authorized state.
force-authorized	Sets the authorization state of the port to Authorized, bypassing the authentication process.
force-unauthorized	Sets the authorization state of the port to Unauthorized, bypassing the authentication process.

no dot1x supplicant port-control

This command sets the port-control mode to the default, auto.

Default	auto
Format	`no dot1x supplicant port-control`
Mode	Interface Config

dot1x supplicant max-start

This command configures the number of attempts that the supplicant makes to find the authenticator before the supplicant assumes that there is no authenticator.

Default	3
Format	`dot1x supplicant max-start` *1-10*
Mode	Interface Config

no dot1x supplicant max-start

This command sets the max-start value to the default.

Format	`no dot1x supplicant max-start`
Mode	Interface Config

dot1x supplicant timeout start-period

This command configures the start period timer interval, in seconds, to wait for the EAP identity request from the authenticator.

Default	30 seconds
Format	`dot1x supplicant timeout start-period` *1-65535*
Mode	Interface Config

no dot1x supplicant timeout start-period

This command sets the start-period value to the default.

Format	`no dot1x supplicant timeout start-period`
Mode	Interface Config

dot1x supplicant timeout held-period

This command configures the held period timer interval, in seconds, to wait for the next authentication on previous authentication fail.

Default	60 seconds
Format	`dot1x supplicant timeout held-period` *`1-65535`*
Mode	Interface Config

no dot1x supplicant timeout held-period

This command sets the held-period value to the default value.

Format	`no dot1x supplicant timeout held-period`
Mode	Interface Config

dot1x supplicant timeout auth-period

This command configures the authentication period timer interval, in seconds, to wait for the next EAP request challenge from the authenticator.

Default	30 seconds
Format	`dot1x supplicant timeout auth-period` *`1-65535`*
Mode	Interface Config

no dot1x supplicant timeout auth-period

This command sets the auth-period value to the default value.

Format	`no dot1x supplicant timeout auth-period`
Mode	Interface Config

dot1x supplicant user

Use this command to map the given user to the port.

Format	`dot1x supplicant user`
Mode	Interface Config

show dot1x statistics

This command displays the dot1x port statistics in detail.

Format	`show dot1x statistics` *`slot/port`*
Mode	• Privileged EXEC • User EXEC

Column	Meaning
EAPOL Frames Received	Displays the number of valid EAPOL frames received on the port.
EAPOL Frames Transmitted	Displays the number of EAPOL frames transmitted via the port.
EAPOL Start Frames Transmitted	Displays the number of EAPOL Start frames transmitted via the port.
EAPOL Logoff Frames Received	Displays the number of EAPOL Log off frames that have been received on the port.
EAP Resp/ID Frames Received	Displays the number of EAP Respond ID frames that have been received on the port.
EAP Response Frames Received	Displays the number of valid EAP Respond frames received on the port.
EAP Req/ID Frames Transmitted	Displays the number of EAP Requested ID frames transmitted via the port.
EAP Req Frames Transmitted	Displays the number of EAP Request frames transmitted via the port.
Invalid EAPOL Frames Received	Displays the number of unrecognized EAPOL frames received on this port.
EAP Length Error Frames Received	Displays the number of EAPOL frames with an invalid Packet Body Length received on this port.
Last EAPOL Frames Version	Displays the protocol version number attached to the most recently received EAPOL frame.
Last EAPOL Frames Source	Displays the source MAC Address attached to the most recently received EAPOL frame.

The following example shows CLI display output for the command.

```
(Extreme 220) #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
```

Task-based Authorization

Task-based authorization allows users to have different permission levels (read, write, execute, debug) at a per-component level. Task-based authorization uses the concept of components/tasks to define permission for commands for a given user.

Users are assigned to User Groups that are, in turn, associated with Task Groups. Each Task Group is then associated with one or more tasks/components. This release supports the AAA, *BGP (Border Gateway Protocol)* and *OSPF (Open Shortest Path First)* components. Also, this feature is supported only for users who are authenticated locally via the CLI interface.

usergroup

This command creates a user group with the specified name and enters user group configuration mode.

Format	`usergroup` *`usergroup-name`*
Mode	Global Config

no usergroup

This command removes the user group with the specified name.

Format	`no usergroup` *`usergroup-name`*
Mode	Global Config

taskgroup

This command creates a task group with the specified name and enters task group configuration mode.

Format	`taskgroup` *`taskgroup-name`*
Mode	Global Config

no taskgroup

This command removes the task group with the specified name.

Format	`no taskgroup` *`taskgroup-name`*
Mode	Global Config

username usergroup

This command assigns the specified user to the specified user group.

Format	`username` *`username`* `usergroup` *`usergroup-name`*
Mode	Global Config

no username usergroup

This command removes the specified user from the specified user group.

Format	`no usergroup` *`usergroup-name`*
Mode	Global Config

description (User Group Mode)

This command sets a description for the user group.

Format	`description` *`description`*
Mode	User Group

no description (User Group Mode)

This command removes the description from the user group.

Format	`no description`
Mode	User Group

inherit usergroup

This command sets the parent user group of the current user group. The user group will have the permissions of the specified parent group.

Format	`inherit usergroup` *`usergroup-name`*
Mode	User Group

no inherit usergroup

This command removes the specified parent group relationship from the user group.

Format	`no inherit usergroup` *`usergroup-name`*
Mode	User Group

taskgroup (User Group Mode)

This command associates the user group with the specified task group.

Format	`taskgroup` *`taskgroup-name`*
Mode	User Group

no taskgroup (User Group Mode)

This command removes the user group's relationship with the associated task group.

Format	`no taskgroup` *`taskgroup-name`*
Mode	User Group

description (Task Group Mode)

This command sets a description for the task group.

Format	`description` *`description`*
Mode	Task Group

no description (Task Group Mode)

This command removes the description from the task group.

Format	`no description`
Mode	Task Group

inherit taskgroup

This command sets the parent task group of the current task group. The task group will have the permissions of the specified parent task group.

Format	`inherit taskgroup` *`taskgroup-name`*
Mode	Task Group

no inherit taskgroup

This command removes the specified parent group relationship from the user group.

Format	`no inherit taskgroup` *`taskgroup-name`*
Mode	Task Group

task [read] [write] [debug] [execute]

This command associates the task group with the specified set of task permissions.

Default	No permissions
Format	`task [read] [write] [debug] [execute]`
Mode	Task Group

The following example gives all users in the task group tg1 read-only permissions for AAA and read, write, execute, and debug permissions for OSPF.

```
(Extreme 220) (Routing) #configure
(Extreme 220) (Config) #taskgroup tg1
(Extreme 220) (config-taskgroup)#task read aaa
(Extreme 220) (config-taskgroup)#task read write execute debug ospf
```

no task [aaa | ospf | bgp]

This command removes all relationships with the associated task.

Format	*no task*
Mode	Task Group

show aaa usergroup

This command displays a list of user groups and their configuration.

Format	show aaa usergroup [*usergroup-name*]
Mode	Privileged EXEC

The following example shows CLI display output for the command.

```
(Extreme 220) (Routing) #show aaa usergroup group1
User group "group1"
Description : "Example"
Parent user groups: “”
Contained task groups:
task group#1: "tg1"
Operational permissions:
Task: aaa                       : READ     WRITE     EXECUTE     DEBUG
Task: ospf                      : READ     WRITE     EXECUTE     DEBUG
Task: bgp                       : READ     WRITE     EXECUTE     DEBUG
```

show aaa taskgroup

This command displays a list of task groups and their configuration.

Format	show aaa taskgroup [*taskgroup-name*]
Mode	Privileged EXEC

The following example shows CLI display output for the command.

```
(Extreme 220) (Routing) #show aaa taskgroup
Task group "default-taskgroup-name"
Description : ""
Parent taskgroups: ""
Configured permissions:
Task: aaa                           : READ     WRITE     EXECUTE     DEBUG
Task: ospf                             : READ     WRITE     EXECUTE     DEBUG
Task: bgp                           : READ     WRITE     EXECUTE     DEBUG
Operational permission:
Task: aaa                           : READ     WRITE     EXECUTE     DEBUG
Task: ospf                             : READ     WRITE     EXECUTE     DEBUG
Task: bgp                           : READ     WRITE     EXECUTE     DEBUG
Task group "task1"
Description : ""
Parent taskgroups: ""
Configured permissions:
Task: aaa                           : READ     WRITE     EXECUTE     DEBUG
Task: ospf                             : READ
```

```
Task: bgp                              : READ
Operational permission:
Task: aaa                              : READ     WRITE     EXECUTE     DEBUG
Task: ospf                               : READ
Task: bgp                              : READ
```

show aaa userdb

This command displays a list of users and list of groups the users participate in.

Format	`show aaa userdb [username]`
Mode	Privileged EXEC

The following example shows CLI display output for the command.

```
(Extreme 220) (Routing) #show aaa userdb admin
User "admin"
Contained user groups:
user group#1 : "ICOS-Root"
Operational permissions:
Task: aaa                          : READ     WRITE     EXECUTE     DEBUG
Task: ospf                         : READ     WRITE     EXECUTE     DEBUG
Task: bgp                          : READ     WRITE     EXECUTE     DEBUG
```

Storm-Control Commands

This section describes commands used 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.

200 Series provides broadcast, multicast, and unicast story recovery for individual interfaces. Unicast Storm-Control protects against traffic whose MAC addresses are not known by the system. For broadcast, multicast, and unicast storm-control, if the rate of traffic ingressing on an interface increases beyond the configured threshold for that type, the traffic is dropped.

To configure storm-control, you will enable the feature for all interfaces or for individual interfaces, and you will set the threshold (storm-control level) beyond which the broadcast, multicast, or unicast traffic will be dropped. The Storm-Control feature allows you to limit the rate of specific types of packets through the switch on a per-port, per-type, basis.

Configuring a storm-control level also enables that form of storm-control. Disabling a storm-control level (using the “no” version of the command) sets the storm-control level back to the default value and disables that form of storm-control. Using the “no” version of the “storm-control” command (not stating

a “level”) disables that form of storm-control but maintains the configured “level” (to be active the next time that form of storm-control is enabled.)

Note

The actual rate of ingress traffic required to activate storm-control is based on the size of incoming packets and the hard-coded average packet size of 512 bytes - used to calculate a packet-per-second (pps) rate - as the forwarding-plane requires pps versus an absolute rate kbps. For example, if the configured limit is 10%, this is converted to ~25000 pps, and this pps limit is set in forwarding plane (hardware). You get the approximate desired output when 512bytes packets are used.

storm-control broadcast

Use this command to enable broadcast storm recovery mode for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode). If the mode is enabled, broadcast storm recovery is active and, if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of broadcast traffic will be limited to the configured threshold.

Default	Disabled
Format	`storm-control broadcast`
Mode	• Global Config • Interface Config

no storm-control broadcast

Use this command to disable broadcast storm recovery mode for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode).

Format	`no storm-control broadcast`
Mode	• Global Config • Interface Config

storm-control broadcast action

This command configures the broadcast storm recovery action to either shutdown or trap for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode). If configured to shutdown, the interface that receives the broadcast packets at a rate above the threshold is diagnostically disabled. If set to trap, the interface sends trap messages approximately every 30 seconds until broadcast storm control recovers.

Default	None
Format	`storm-control broadcast action {shutdown | trap}`
Mode	• Global Config • Interface Config

no storm-control broadcast action

This command configures the broadcast storm recovery action option to the default value for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode).

Format	`no storm-control broadcast action`
Mode	• Global Config • Interface Config

storm-control broadcast level

Use this command to configure the broadcast storm recovery threshold for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) as a percentage of link speed and enable broadcast storm recovery. If the mode is enabled, broadcast storm recovery is active, and if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic is dropped. Therefore, the rate of broadcast traffic is limited to the configured threshold.

Default	5
Format	`storm-control broadcast level` *`0-100`*
Mode	• Global Config • Interface Config

no storm-control broadcast level

This command sets the broadcast storm recovery threshold to the default value for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) and disables broadcast storm recovery.

Format	`no storm-control broadcast level`
Mode	• Global Config • Interface Config

storm-control broadcast rate

Use this command to configure the broadcast storm recovery threshold for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) in packets per second. If the mode is enabled, broadcast storm recovery is active, and if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic is dropped. Therefore, the rate of broadcast traffic is limited to the configured threshold.

Default	0
Format	`storm-control broadcast rate` *`0-33554431`*
Mode	• Global Config • Interface Config

no storm-control broadcast rate

This command sets the broadcast storm recovery threshold to the default value for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) and disables broadcast storm recovery.

Format	`no storm-control broadcast rate`
Mode	• Global Config • Interface Config

storm-control multicast

This command enables multicast storm recovery mode for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode). If the mode is enabled, multicast storm recovery is active, and if the rate of L2 multicast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of multicast traffic will be limited to the configured threshold.

Default	Disabled
Format	`storm-control multicast`
Mode	• Global Config • Interface Config

no storm-control multicast

This command disables multicast storm recovery mode for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode).

Format	`no storm-control multicast`
Mode	• Global Config • Interface Config

storm-control multicast action

This command configures the multicast storm recovery action to either shutdown or trap for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode). If configured to shutdown, the interface that receives multicast packets at a rate above the threshold is diagnostically disabled. The option **`trap`** sends trap messages approximately every 30 seconds until multicast storm control recovers.

Default	None
Format	`storm-control multicast action {shutdown | trap}`
Mode	• Global Config • Interface Config

no storm-control multicast action

This command returns the multicast storm recovery action option to the default value for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode).

Format	`no storm-control multicast action`
Mode	• Global Config • Interface Config

storm-control multicast level

This command configures the multicast storm recovery threshold for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) as a percentage of link speed and enables multicast storm recovery mode. If the mode is enabled, multicast storm recovery is active, and if the rate of L2 multicast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of multicast traffic will be limited to the configured threshold.

Default	5
Format	`storm-control multicast level` *`0-100`*
Mode	• Global Config • Interface Config

no storm-control multicast level

This command sets the multicast storm recovery threshold to the default value for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) and disables multicast storm recovery.

Format	`no storm-control multicast level` *`0-100`*
Mode	• Global Config • Interface Config

storm-control multicast rate

Use this command to configure the multicast storm recovery threshold for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) in packets per second. If the mode is enabled, multicast storm recovery is active, and if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic is dropped. Therefore, the rate of multicast traffic is limited to the configured threshold.

Default	0
Format	`storm-control multicast rate` *`0-33554431`*
Mode	• Global Config • Interface Config

no storm-control multicast rate

This command sets the multicast storm recovery threshold to the default value for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) and disables multicast storm recovery.

Format	`no storm-control multicast rate`
Mode	• Global Config • Interface Config

storm-control unicast

This command enables unicast storm recovery mode for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode). If the mode is enabled, unicast storm recovery is active, and if the rate of unknown L2 unicast (destination lookup failure) traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of unknown unicast traffic will be limited to the configured threshold.

Default	Disabled
Format	`storm-control unicast`
Mode	• Global Config • Interface Config

no storm-control unicast

This command disables unicast storm recovery mode for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode).

Format	`no storm-control unicast`
Mode	• Global Config • Interface Config

storm-control unicast action

This command configures the unicast storm recovery action to either shutdown or trap for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode). If configured to shutdown, the interface that receives unicast packets at a rate above the threshold is diagnostically disabled. The option **`trap`** sends trap messages approximately every 30 seconds until unicast storm control recovers.

Default	None
Format	`storm-control unicast action {shutdown | trap}`
Mode	• Global Config • Interface Config

no storm-control unicast action

This command returns the unicast storm recovery action option to the default value for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode).

Format	`no storm-control unicast action`
Mode	• Global Config • Interface Config

storm-control unicast level

This command configures the unicast storm recovery threshold for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) as a percentage of link speed, and enables unicast storm recovery. If the mode is enabled, unicast storm recovery is active, and if the rate of unknown L2 unicast (destination lookup failure) traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of unknown unicast traffic will be limited to the configured threshold.This command also enables unicast storm recovery mode for an interface.

Default	5
Format	`storm-control unicast level` *`0-100`*
Mode	• Global Config • Interface Config

no storm-control unicast level

This command sets the unicast storm recovery threshold to the default value for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) and disables unicast storm recovery.

Format	`no storm-control unicast level`
Mode	• Global Config • Interface Config

storm-control unicast rate

Use this command to configure the unicast storm recovery threshold for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) in packets per second. If the mode is enabled, unicast storm recovery is active, and if the rate of L2 broadcast traffic ingressing on an interface

increases beyond the configured threshold, the traffic is dropped. Therefore, the rate of unicast traffic is limited to the configured threshold.

Default	0
Format	`storm-control unicast rate` *`0-33554431`*
Mode	• Global Config • Interface Config

no storm-control unicast rate

This command sets the unicast storm recovery threshold to the default value for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) and disables unicast storm recovery.

Format	`no storm-control unicast rate`
Mode	• Global Config • Interface Config

show storm-control

This command displays switch configuration information. If you do not use any of the optional parameters, this command displays global storm control configuration parameters:

- Broadcast Storm Recovery Mode may be enabled or disabled. The factory default is disabled.
- 802.3x Flow Control Mode may be enabled or disabled. The factory default is disabled.

Use the **`all`** keyword to display the per-port configuration parameters for all interfaces, or specify the unit/slot/port to display information about a specific interface.

Format	`show storm-control [all |` *`unit/slot/port`*`]`
Mode	Privileged EXEC

Column	Meaning
Bcast Mode	Shows whether the broadcast storm control mode is enabled or disabled. The factory default is disabled.
Bcast Level	The broadcast storm control level.
Mcast Mode	Shows whether the multicast storm control mode is enabled or disabled.
Mcast Level	The multicast storm control level.
Ucast Mode	Shows whether the Unknown Unicast or DLF (Destination Lookup Failure) storm control mode is enabled or disabled.
Ucast Level	The Unknown Unicast or DLF (Destination Lookup Failure) storm control level.

The following example shows CLI display output for the command.

```
(Extreme 220) (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
```

The following example shows CLI display output for the command.

```
(Extreme 220) (Routing) #show storm-control 1/0/1
       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
```

The following shows an example of part of the CLI display output for the command.

```
(Extreme 220) (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  50        Trap       Disable 5%       None       Disable 5%       None
1/0/2  Enable  50        Trap       Disable 5%       None       Disable 5%       None
1/0/3  Enable  50        Trap       Disable 5%       None       Disable 5%       None
1/0/4  Enable  50        Trap       Disable 5%       None       Disable 5%       None
1/0/5  Enable  50        Trap       Disable 5%       None       Disable 5%       None
1/0/6  Enable  50        Trap       Disable 5%       None       Disable 5%       None
1/0/7  Enable  50        Trap       Disable 5%       None       Disable 5%       None
1/0/8  Enable  50        Trap       Disable 5%       None       Disable 5%       None
1/0/9  Enable  50        Trap       Disable 5%       None       Disable 5%       None
1/0/10 Enable  50        Trap       Disable 5%       None       Disable 5%       None
1/0/11 Enable  50        Trap       Disable 5%       None       Disable 5%       None
1/0/12 Enable  50        Trap       Disable 5%       None       Disable 5%       None
1/0/13 Enable  50        Trap       Disable 5%       None       Disable 5%       None
1/0/14 Enable  50        Trap       Disable 5%       None       Disable 5%       None
1/0/15 Enable  50        Trap       Disable 5%       None       Disable 5%       None
1/0/16 Enable  50        Trap       Disable 5%       None       Disable 5%       None
1/0/17 Enable  50        Trap       Disable 5%       None       Disable 5%       None
1/0/18 Enable  50        Trap       Disable 5%       None       Disable 5%       None
1/0/19 Enable  50        Trap       Disable 5%       None       Disable 5%       None
```

Link Dependency Commands

The following commands configure link dependency. Link dependency allows the link status of specified ports to be dependent on the link status of other ports. Consequently, if a port that is depended on by other ports loses link, the dependent ports are administratively disabled or administratively enabled so that the dependent ports links are brought down or up respectively.

no link state track

This command clears link-dependency options for the selected group identifier.

Format	`no link state track` *group-id*
Mode	Global Config

link state group

Use this command to indicate if the downstream interfaces of the group should mirror or invert the status of the upstream interfaces. The default configuration for a group is down (that is, the downstream interfaces will mirror the upstream link status by going down when all upstream interfaces are down). The action up option causes the downstream interfaces to be up when no upstream interfaces are down.

Default	down
Format	`link state group` *`group-id`* `action {up | down}`
Mode	Global Config

no link state group

Use this command to restore the link state to down for the group.

Format	`no link state group` *`group-id`* `action`
Mode	Global Config

link state group downstream

Use this command to add interfaces to the downstream interface list. Adding an interface to a downstream list brings the interface down until an upstream interface is added to the group. The link status then follows the interface specified in the upstream command. To avoid bringing down interfaces, enter the upstream command prior to entering the downstream command.

Format	`link state group` *`group-id`* `downstream`
Mode	Interface Config

no link state group downstream

Use this command to remove the selected interface from the downstream list.

Format	`no link state group` *`group-id`* `downstream`
Mode	Interface Config

link state group upstream

Use this command to add interfaces to the upstream interface list. Note that an interface that is defined as an upstream interface cannot also be defined as a downstream interface in the same link state group or as a downstream interface in a different link state group, if either configuration creates a circular dependency between groups.

Format	`link state group` *`group-id`* `upstream`
Mode	Interface Config

no link state group upstream

Use this command to remove the selected interfaces from upstream list.

Format	`no link state group` *`group-id`* `upstream`
Mode	Interface Config

show link state group

Use this command to display information for all configured link-dependency groups or a specified link-dependency group.

Format	`show link state group` *`group-id`*
Mode	Privileged EXEC

This example displays information for all configured link-dependency groups.

```
(Extreme 220)#show link-state group
GroupId Downstream Interfaces      Upstream Interfaces  Link Action Group State
------- -------------------------- -------------------- ----------- -----------
1       2/0/3-2/0/7,2/0/12-2/0/17  2/0/12-2/0/32,0/3/5  Link Up     Up
4       2/0/18,2/0/27              2/0/22-2/0/33,0/3/1  Link Up     Down
```

This example displays information for a specified link-dependency groups

```
(Extreme 220)#show link state group 1
GroupId Downstream Interfaces      Upstream Interfaces  Link Action Group State
------- -------------------------- -------------------- ----------- -----------
1       2/0/3-2/0/7,2/0/12-2/0/17  2/0/12-2/0/32,0/3/5  Link Up     Up
```

show link state group detail

Use this command to display detailed information about the state of upstream and downstream interfaces for a selected link-dependency group. Group Transitions is a count of the number of times the downstream interface has gone into its “action” state as a result of the upstream interfaces link state.

Format	`show link state group` *`group-id`* `detail`
Mode	Privileged EXEC

```
(Extreme 220) #show link state group 1 detail
GroupId:     1
Link Action: Up
Group State: Up
Downstream Interface State:
Link Up:     2/0/3
Link Down:   2/0/4-2/0/7,2/0/12-2/0/17
Upstream Interface State:
Link Up:     -
Link Down:  2/0/12-2/0/32,0/3/5
Group Transitions: 0
Last Transition Time: 00:52:35 (UTC+0:00) Jan 1 1970
```

Port-Channel/LAG (802.3ad) Commands

This section describes the commands used to configure port-channels, which is defined in the 802.3ad specification, and that are also known as *LAG*s. Link aggregation allows you to combine multiple full-duplex Ethernet links into a single logical link. Network devices treat the aggregation as if it were a single link, which increases fault tolerance and provides load sharing. The LAG feature initially load shares traffic based upon the source and destination MAC address. Assign the port-channel (LAG) VLAN membership after you create a port-channel. If you do not assign VLAN membership, the port-channel might become a member of the management VLAN which can result in learning and switching issues.

A port-channel (LAG) interface can be either static or dynamic, but not both. All members of a port channel must participate in the same protocols.) A static port-channel interface does not require a partner system to be able to aggregate its member ports.

Note
If you configure the maximum number of dynamic port-channels (LAGs) that your platform supports, additional port-channels that you configure are automatically static.

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 "-" character as well as alphanumeric characters. Use the `show port channel` command to display the unit/slot/port number for the logical interface. 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.

Note
Before you include a port in a port-channel, set the port physical mode. For more information, see speed on page 281.

Format	`port-channel` *`name`*
Mode	Global Config

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 (for example: interface 1/0/1-1/0/4. 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.

Note
Before adding a port to a port-channel, set the physical mode of the port. For more information, see speed on page 281.

Format	`addport`*`unit/slot/port`*
Mode	Interface Config

deleteport (Interface Config)

This command deletes a port or a range of ports from the port-channel (*LAG*). The interface is a logical unit/slot/port number of a configured port-channel (or range of port-channels). 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.

Format	`deleteport` *`unit/slot/port`*
Mode	Interface Config

deleteport (Global Config)

This command deletes all configured ports from the port-channel (*LAG*). The interface is a logical unit/slot/port number of a configured port-channel. 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.

Format	`deleteport {`*`unit/slot/port`* `| all}`
Mode	Global Config

lacp admin key

Use this command to configure the administrative value of the key for the port-channel. The value range of key is 0 to 65535.

Default	0x8000
Format	`lacp admin key` *`key`*
Mode	Interface Config

This command can be used to configure a single interface or a range of interfaces.

Note
This command is applicable only to port-channel interfaces.

no lacp admin key

Use this command to configure the default administrative value of the key for the port-channel.

Format	`no lacp admin key`
Mode	Interface Config

lacp collector max-delay

Use this command to configure the port-channel collector max delay. This command can be used to configure a single interface or a range of interfaces. The valid range of delay is 0-65535.

Default	0x8000
Format	`lacp collector max delay` *`delay`*
Mode	Interface Config

Note
This command is applicable only to port-channel interfaces.

no lacp collector max delay

Use this command to configure the default port-channel collector max delay.

Format	`no lacp collector max delay`
Mode	Interface Config

lacp actor admin key

Use this command to configure the administrative value of the LACP actor admin key on an interface or range of interfaces. The valid range for key is 0-65535.

Default	Internal Interface Number of this Physical Port
Format	`lacp actor admin key` *`key`*
Mode	Interface Config

Note
This command is applicable only to physical interfaces.

no lacp actor admin key

Use this command to configure the default administrative value of the key.

Format	`no lacp actor admin key`
Mode	Interface Config

lacp actor admin state individual

Use this command to set LACP actor admin state to individual.

Format	`lacp actor admin state individual`
Mode	Interface Config

Note
This command is applicable only to physical interfaces.

no lacp actor admin state individual

Use this command to set the LACP actor admin state to aggregation.

Format	`no lacp actor admin state individual`
Mode	Interface Config

lacp actor admin state longtimeout

Use this command to set LACP actor admin state to longtimeout.

Format	`lacp actor admin state longtimeout`
Mode	Interface Config

Note
This command is applicable only to physical interfaces.

no lacp actor admin state longtimeout

Use this command to set the LACP actor admin state to short timeout.

Format	`no lacp actor admin state longtimeout`
Mode	Interface Config

Note
This command is applicable only to physical interfaces.

lacp actor admin state passive

Use this command to set the LACP actor admin state to passive.

Format	`lacp actor admin state passive`
Mode	Interface Config

Note
This command is applicable only to physical interfaces.

no lacp actor admin state passive

Use this command to set the LACP actor admin state to active.

Format	`no lacp actor admin state passive`
Mode	Interface Config

lacp actor admin state

Use this command to configure the administrative value of actor state as transmitted by the Actor in LACPDUs. This command can be used to configure a single interfaces or a range of interfaces.

Default	0x07
Format	`lacp actor admin state {individual|longtimeout|passive}`
Mode	Interface Config

Note
This command is applicable only to physical interfaces.

no lacp actor admin state

Use this command the configure the default administrative values of actor state as transmitted by the Actor in LACPDUs.

Note
Both the no portlacptimeout and the `no lacp actor admin state` commands set the values back to default, regardless of the command used to configure the ports. Consequently, both commands will display in show running-config.

Format	`no lacp actor admin state {individual|longtimeout|passive}`
Mode	Interface Config

lacp actor port priority

Use this command to configure the priority value assigned to the Aggregation Port for an interface or range of interfaces. The valid range for priority is 0 to 65535.

Default	0x80
Format	`lacp actor port priority` *`0-65535`*
Mode	Interface Config

Note
This command is applicable only to physical interfaces.

no lacp actor port priority

Use this command to configure the default priority value assigned to the Aggregation Port.

Format	`no lacp actor port priority`
Mode	Interface Config

lacp partner admin key

Use this command to configure the administrative value of the Key for the protocol partner. This command can be used to configure a single interface or a range of interfaces. The valid range for key is 0 to 65535.

Default	0x0
Format	`lacp partner admin key` *`key`*
Mode	Interface Config

Note
This command is applicable only to physical interfaces.

no lacp partner admin key

Use this command to set the administrative value of the Key for the protocol partner to the default.

Format	`no lacp partner admin key`
Mode	Interface Config

lacp partner admin state individual

Use this command to set LACP partner admin state to individual.

Format	`lacp partner admin state individual`
Mode	Interface Config

Note
This command is applicable only to physical interfaces.

no lacp partner admin state individual

Use this command to set the LACP partner admin state to aggregation.

Format	`no lacp partner admin state individual`
Mode	Interface Config

lacp partner admin state longtimeout

Use this command to set LACP partner admin state to longtimeout.

Format	`lacp partner admin state longtimeout`
Mode	Interface Config

Note
This command is applicable only to physical interfaces.

no lacp partner admin state longtimeout

Use this command to set the LACP partner admin state to short timeout.

Format	`no lacp partner admin state longtimeout`
Mode	Interface Config

Note
This command is applicable only to physical interfaces.

lacp partner admin state passive

Use this command to set the LACP partner admin state to passive.

Format	`lacp partner admin state passive`
Mode	Interface Config

Note
This command is applicable only to physical interfaces.

no lacp partner admin state passive

Use this command to set the LACP partner admin state to active.

Format	`no lacp partner admin state passive`
Mode	Interface Config

lacp partner port id

Use this command to configure the LACP partner port id. This command can be used to configure a single interface or a range of interfaces. The valid range for *`port-id`* is 0 to 65535.

Default	0x80
Format	`lacp partner port id` *`port-id`*
Mode	Interface Config

Note
This command is applicable only to physical interfaces.

no lacp partner port id

Use this command to set the LACP partner port id to the default.

Format	`no lacp partner port-id`
Mode	Interface Config

lacp partner port priority

Use this command to configure the LACP partner port priority. This command can be used to configure a single interface or a range of interfaces. The valid range for priority is 0 to 65535.

Default	0x0
Format	`lacp partner port priority` *`priority`*
Mode	Interface Config

Note
This command is applicable only to physical interfaces.

no lacp partner port priority

Use this command to configure the default LACP partner port priority.

Format	`no lacp partner port priority`
Mode	Interface Config

lacp partner system id

Use this command to configure the 6-octet MAC Address value representing the administrative value of the Aggregation Port's protocol Partner's System ID. This command can be used to configure a single interface or a range of interfaces. The valid range of system-id is 00:00:00:00:00:00 - FF:FF:FF:FF:FF:FF.

Default	00:00:00:00:00:00
Format	`lacp partner system id` *`system-id`*
Mode	Interface Config

Note
This command is applicable only to physical interfaces.

no lacp partner system id

Use this command to configure the default value representing the administrative value of the Aggregation Port's protocol Partner's System ID.

Format	`no lacp partner system id`
Mode	Interface Config

lacp partner system priority

Use this command to configure the administrative value of the priority associated with the Partner's System ID. This command can be used to configure a single interface or a range of interfaces. The valid range for priority is 0 to 65535.

Default	0x0
Format	`lacp partner system priority` *`0-65535`*
Mode	Interface Config

Note
This command is applicable only to physical interfaces.

no lacp partner system priority

Use this command to configure the default administrative value of priority associated with the Partner's System ID.

Format	`no lacp partner system priority`
Mode	Interface Config

interface lag

Use this command to enter Interface configuration mode for the specified *LAG*.

Format	`interface lag` *`lag-interface-number`*
Mode	Global Config

port-channel static

This command enables the static mode on a port-channel (*LAG*) interface or range of interfaces. By default the static mode for a new port-channel is enabled, which means the port-channel is static. If the maximum number of allowable dynamic port-channels are already present in the system, the static mode for a new port-channel is enabled, which means the port-channel is static. You can only use this command on port-channel interfaces.

Default	Enabled
Format	`port-channel static`
Mode	Interface Config

no port-channel static

This command sets the static mode on a particular port-channel (*LAG*) interface to the default value. This command will be executed only for interfaces of type port-channel (LAG).

Format	`no port-channel static`
Mode	Interface Config

port lacpmode

This command enables Link Aggregation Control Protocol (LACP) on a port or range of ports.

Default	Enabled
Format	`port lacpmode`
Mode	Interface Config

no port lacpmode

This command disables Link Aggregation Control Protocol (LACP) on a port.

Format	`no port lacpmode`
Mode	Interface Config

port lacpmode enable all

This command enables Link Aggregation Control Protocol (LACP) on all ports.

Format	`port lacpmode enable all`
Mode	Global Config

no port lacpmode enable all

This command disables Link Aggregation Control Protocol (LACP) on all ports.

Format	`no port lacpmode enable all`
Mode	Global Config

port lacptimeout (Interface Config)

This command sets the timeout on a physical interface or range of interfaces of a particular device type (actor or partner) to either long or short timeout.

Default	long
Format	`port lacptimeout {actor | partner} {long | short}`
Mode	Interface Config

no port lacptimeout

This command sets the timeout back to its default value on a physical interface of a particular device type (actor or partner).

Format	`no port lacptimeout {actor | partner}`
Mode	Interface Config

Note

Both the no portlacptimeout and the `no lacp actor admin state` commands set the values back to default, regardless of the command used to configure the ports. Consequently, both commands will display in show running-config.

port lacptimeout (Global Config)

This command sets the timeout for all interfaces of a particular device type (actor or partner) to either long or short timeout.

Default	long
Format	`port lacptimeout {actor | partner} {long | short}`
Mode	Global Config

no port lacptimeout

This command sets the timeout for all physical interfaces of a particular device type (actor or partner) back to their default values.

Format	`no port lacptimeout {actor | partner}`
Mode	Global Config

Note

Both the no portlacptimeout and the `no lacp actor admin state` commands set the values back to default, regardless of the command used to configure the ports. Consequently, both commands will display in show running-config.

port-channel adminmode

This command enables all configured port-channels with the same administrative mode setting.

Format	`port-channel adminmode all`
Mode	Global Config

no port-channel adminmode

This command disables all configured port-channels with the same administrative mode setting.

Format	`no port-channel adminmode all`
Mode	Global Config

port-channel linktrap

This command enables link trap notifications for the port-channel (*LAG*). The interface is a logical unit/slot/port for a configured port-channel. The option all sets every configured port-channel with the same administrative mode setting. 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.

Default	Enabled
Format	`port-channel linktrap {`*`logical unit/slot/port`*` | all}`
Mode	Global Config

no port-channel linktrap

This command disables link trap notifications for the port-channel (*LAG*). The interface is a logical slot and port for a configured port-channel. The option all sets every configured port-channel with the same administrative mode setting.

Format	`no port-channel linktrap {`*`logical unit/slot/port`*` | all}`
Mode	Global Config

port-channel load-balance

This command selects the load-balancing option used on a port-channel (*LAG*). Traffic is balanced on a port-channel (LAG) by selecting one of the links in the channel over which to transmit specific packets. The link is selected by creating a binary pattern from selected fields in a packet, and associating that pattern with a particular link.

Load-balancing is not supported on every device. The range of options for load-balancing may vary per device.

This command can be configured for a single interface, a range of interfaces, or all interfaces. Instead of 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.

Default	3
Format	`port-channel load-balance {1 | 2 | 3 | 4 | 5 | 6 | 7} {`*`unit/slot/port`* `| all}`
Mode	Interface Config Global Config

Parameter	Description
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. The keyword**all** applies the command to all currently configured port-channels.

no port-channel load-balance

This command reverts to the default load balancing configuration.

Format	`no port-channel load-balance {`*`unit/slot/port`* `| all}`
Mode	Interface Config Global Config

Term	Definition
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.

port-channel min-links

This command configures the port-channel's minimum links for lag interfaces.

Default	1
Format	`port-channel min-links 1-8`
Mode	Interface Config

port-channel name

This command defines a name for the port-channel (*LAG*). The interface is a logical unit/slot/port for a configured port-channel, and name is an alphanumeric string up to 15 characters. 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.

Format	`port-channel name {unit/slot/port} name`
Mode	Global Config

port-channel system priority

Use this command to configure port-channel system priority. The valid range of priority is 0-65535.

Default	0x8000
Format	`port-channel system priority priority`
Mode	Global Config

no port-channel system priority

Use this command to configure the default port-channel system priority value.

Format	`no port-channel system priority`
Mode	Global Config

show hashdest

Use this command to predict how packets are forwarded over a *LAG* or to the next hop device when *ECMP (Equal Cost Multi Paths)* is the destination. Given the link aggregation method, ingress physical port and values of various packet fields, this command predicts an egress physical port within the LAG or ECMP for the packet.

Format	`show hashdest {lag lag-id | ecmp prefix/prefix-length} in_port unit/slot/port src-mac macaddr dst-mac macaddr [vlan vlan-id] ethertype 0xXXXX [src-ip {ipv4-addr | ipv6-addr} dst-ip {ipv4-addr | ipv6-addr} protocol pid src-l4-port port-num dst-l4-port port-num]`
Mode	Privileged EXEC

Parameter	Definition
lag	The LAG group for which to display the egress physical port.
ecmp	The IP address of the EMC_ group for which to display the egress physical port.
in_port	The incoming physical port for the system.
src-mac	The source MAC address.
dst-mac	The destination MAC address.
vlan	The VLAN ID for VLAN-tagged packets. Do not use this parameter or enter 0 for non-VLAN-tagged packets.
ethertype	The 16-bit EtherType value, in the form *0xXXXX*. For layer 3 packets, hash prediction is only available for IPv4 (0x0800) and IPv6 (0x86DD).
src-ip	The source IP address, entered as *x.x.x.x* for IPv4 or *x:x:x:x:x:x:x:x* for IPv6 packets.
dst-ip	The destination IP address, entered as *x.x.x.x* for IPv4 or *x:x:x:x:x:x:x:x* for IPv6 packets.
protocol	The protocol ID.
src-l4-port	The layer 4 source port.
dst-l4-port	The layer 4 destination port.

Layer 2 VLAN tagged packet forwarded to a LAG

```
(Extreme 220) (Routing) #show hashdest lag 1 in_port 0/3 src-mac 00:00:20:21:AE:8A dst-mac
00:10:18:99:F7:4E vlan 10 ethertype 0x8870
LAG            Destination Port
-----------     ----------------
1                  0/29
```

Layer 2 non-VLAN tagged packet forwarded to a LAG

```
(Extreme 220) (Routing) #show hashdest lag 1 in_port 0/3 src-mac 00:00:20:21:AE:8A dst-mac
00:10:18:99:F7:4E ethertype 0x8870
LAG           Destination Port
-----------     ----------------
1            0/31
```

Non-VLAN tagged IPv4 UDP packet forwarded to a LAG

```
(Extreme 220) (Routing) #show hashdest lag 1 in_port 0/3 src-mac 00:00:20:21:AE:8A dst-mac
00:10:18:99:F7:4E ethertype 0x0800 src-ip 7.0.0.2 dst-ip 3.0.0.2 protocol 17 src-l4-port
63 dst-l4-port 64
LAG            Destination Port
-----------     ----------------
1                  0/32
```

VLAN tagged IPv4 TCP packet forwarded to a LAG

```
(Extreme 220) (Routing) #show hashdest lag 1 in_port 0/3 src-mac 00:00:20:21:AE:8A dst-mac
00:10:18:99:F7:4E vlan 10 ethertype 0x0800 src-ip 7.0.0.2 dst-ip 3.0.0.2 protocol 6 src-l4-
port 67 dst-l4-port 68
LAG           Destination Port
-----------     ----------------
1                 0/31
```

Non-VLAN tagged IPv4 UDP packet forwarded to an ECMP group

```
(Extreme 220) (Routing) #show hashdest ecmp  10.0.0.2/16 in_port 0/3 src-mac
00:00:20:21:AE:8A dst-mac 00:10:18:99:F7:4E vlan 0 ethertype 0x0800 src-ip 7.0.0.2 dst-ip
3.0.0.2 protocol 17 src-l4-port 63 dst-l4-port 64
Egress Port
----------------------------
30.0.0.2 on interface 0/31
```

VLAN tagged IPv4 TCP packet forwarded to an ECMP group

```
(Extreme 220) (Routing) #show hashdest ecmp 10.0.0.2/16 in_port 0/3 src-mac 00:00:20:21:AE:
8A dst-mac 00:10:18:99:F7:4E vlan 10 ethertype 0x0800 src-ip 7.0.0.2 dst-ip 3.0.0.2
protocol 6 src-l4-port 67 dst-l4-port 68
Egress Port
-----------
0/29
```

Non-VLAN tagged IPv6 UDP packet forwarded to an ECMP group

```
(Extreme 220) (Routing) #show hashdest ecmp 4001::200/64 in_port 0/3 src-mac
00:00:20:21:AE:8A dst-mac 00:10:18:99:F7:4E ethertype 0x86dd src-ip 7001:0:0:0:0:0:0:2 dst-
ip 3001:0:0:0:0:0:0:2 protocol 17 src-l4-port 63 dst-l4-port 64
Egress Port
----------------------------
6001::200 on interface 0/31
```

Non-VLAN tagged IPv6 TCP packet forwarded to an ECMP group

```
(Extreme 220) (Routing) #show hashdest ecmp 6001::200/64 in_port 0/3 src-mac
00:00:20:21:AE:8A dst-mac 00:10:18:99:F7:4E ethertype 0x86dd src-ip 7001:0:0:0:0:0:0:2 dst-
ip 3001:0:0:0:0:0:0:2 protocol 6 src-l4-port 67 dst-l4-port 68
Egress Port
----------------------------
8001::200 on interface 0/32
```

show lacp actor

Use this command to display LACP actor attributes. 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.

Format	`show lacp actor {`*`unit/slot/port`*`|all}`
Mode	Global Config

The following output parameters are displayed.

Column	Meaning
System Priority	The administrative value of the Key.
Actor Admin Key	The administrative value of the Key.
Port Priority	The priority value assigned to the Aggregation Port.
Admin State	The administrative values of the actor state as transmitted by the Actor in LACPDUs.

show lacp partner

Use this command to display LACP partner attributes. 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.

Format	`show lacp actor {`*`unit/slot/port`*`|all}`
Mode	Privileged EXEC

The following output parameters are displayed.

Column	Meaning
System Priority	The administrative value of priority associated with the Partner's System ID.
System-ID	Represents the administrative value of the Aggregation Port's protocol Partner's System ID.
Admin Key	The administrative value of the Key for the protocol Partner.
Port Priority	The administrative value of the Key for protocol Partner.
Port-ID	The administrative value of the port number for the protocol Partner.
Admin State	The administrative values of the actor state for the protocol Partner.

show port-channel brief

This command displays the static capability of all port-channel (*LAG*) interfaces on the device as well as a summary of individual port-channel interfaces. 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.

Format	`show port-channel brief`
Mode	• User EXEC

For each port-channel the following information is displayed:

Column	Meaning
Logical Interface	The *`unit/slot/port`* of the logical interface.
Port-channel Name	The name of port-channel (LAG) interface.
Link-State	Shows whether the link is up or down.
Trap Flag	Shows whether trap flags are enabled or disabled.
Type	Shows whether the port-channel is statically or dynamically maintained.

Column	Meaning
Mbr Ports	The members of this port-channel.
Active Ports	The ports that are actively participating in the port-channel.

show port-channel

This command displays an overview of all port-channels (*LAG*s) 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.

Format	`show port-channel`
Mode	• Privileged EXEC

Column	Meaning
Logical 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	Whether the Link is up or down.
Admin Mode	May be enabled or disabled. The factory default is enabled.
Type	The status designating whether a particular port-channel (LAG) is statically or dynamically maintained. • Static - The port-channel is statically maintained. • Dynamic - The port-channel is dynamically maintained.
Load Balance Option	The load balance option associated with this LAG. See port-channel load-balance on page 395.
Local Preference Mode	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).

The following example shows CLI display output for the command.

```
(Extreme 220) #show port-channel 0/3/1
Local Interface................................ 0/3/1
Channel Name................................... ch1
Link State..................................... Up
Admin Mode..................................... Enabled
Type........................................... Static
Load Balance Option............................ 3
(Src/Dest MAC, VLAN, EType, incoming port)
Local Preference Mode.......................... Enabled
Mbr    Device/       Port      Port
Ports  Timeout       Speed     Active
------ ------------- --------- -------
1/0/1  actor/long    Auto      True
```

```
       partner/long
1/0/2  actor/long    Auto      True
       partner/long
1/0/3  actor/long    Auto      False
       partner/long
1/0/4  actor/long    Auto      False
       partner/long
```

show port-channel system priority

Use this command to display the port-channel system priority.

Format	`show port-channel system priority`
Mode	Privileged EXEC

show port-channel counters

Use this command to display port-channel counters for the specified port.

Format	`show port-channel` *`unit/slot/port`* `counters`
Mode	Privileged EXEC

Column	Meaning
Local Interface	The valid slot/port number.
Channel Name	The name of this port-channel (*LAG*).
Link State	Whether the Link is up or down.
Admin Mode	May be enabled or disabled. The factory default is enabled.
Port Channel Flap Count	The number of times the port-channel was inactive.
Mbr Ports	The slot/port for the port member.
Mbr Flap Counters	The number of times a port member is inactive, either because the link is down, or the admin state is disabled.

The following example shows CLI display output for the command.

```
(Extreme 220) #show port-channel 3/1 counters
Local Interface............................... 3/1
Channel Name.................................. ch1
Link State.................................... Down
Admin Mode.................................... Enabled
Port Channel Flap Count....................... 0
Mbr    Mbr Flap
Ports  Counters
------ ---------
0/1    0
0/2    0
0/3    1
0/4    0
0/5    0
0/6    0
```

```
0/7     0
0/8     0
```

clear port-channel counters

Use this command to clear and reset specified port-channel and member flap counters for the specified interface.

Format	`clear port-channel {lag-intf-num | unit/slot/port} counters`
Mode	Privileged EXEC

clear port-channel all counters

Use this command to clear and reset all port-channel and member flap counters for the specified interface.

Format	`clear port-channel all counters`
Mode	Privileged EXEC

Port Mirroring Commands

Port mirroring, which is also known as port monitoring, selects network traffic that you can analyze with a network analyzer, such as a SwitchProbe device or other Remote Monitoring (RMON) probe.

monitor session source

This command configures the source interface for a selected monitor session. 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.

Note
The source and destination cannot be configured as remote on the same device.

The port mirroring commands add a mirrored port (source port) to a session identified with session-id. The session-id parameter is an integer value used to identify the session. The maximum number of sessions which can be configured is L7_MIRRORING_MAX_SESSIONS. Option rx is used to monitor only ingress packets. Option tx is used to monitor only egress packets. If no option is specified, both ingress and egress packets, RX and TX, are monitored.

A VLAN can also be configured as the source to a session (all the member ports of that VLAN are monitored).

Note

If an interface participates in some VLAN and is a *LAG* member, this VLAN cannot be assigned as a source VLAN for a Monitor session. At the same time, if an interface participates in some VLAN and this VLAN is assigned as a source VLAN for a Monitor session, the interface can be assigned as a LAG member.

Remote port mirroring is configured by giving the RSPAN VLAN ID. At the source switch the destination is configured as RSPAN VLAN and at the destination switch the source is configured as RSPAN VLAN.

Note

On the intermediate switch, RSPAN VLAN should be created, the ports connected towards Source and Destination switch should have the RSPAN VLAN participation. RSPAN VLAN egress tagging should be enabled on the interface on the intermediate switch connected towards the Destination switch.

Default	None
Format	`monitor session` *`session-id`* `source {interface {`*`unit/slot/port`* `| cpu	lag }	vlan` *`vlan-id`* `| remote vlan` *`vlan-id`* `}[{rx	tx}]`
Mode	Global Config

no monitor session source

This command removes the specified mirrored port from the selected port mirroring session.

Default	None
Format	`no monitor session` *`session-id`* `source {interface {`*`unit/slot/port`* `| cpu	lag }	vlan	remote vlan}`
Mode	Global Config

monitor session destination

This command configures the probe interface for a selected monitor session. This command configures a probe port and a monitored port for monitor session (port monitoring). Use rx to monitor only ingress packets, or use tx to monitor only egress packets. If you do not specify an {rx | tx} option, the destination port monitors both ingress and egress packets.

A VLAN can be configured as the source to a session (all member ports of that VLAN are monitored). Remote port mirroring is configured by adding the RSPAN VLAN ID. At the source switch, the destination is configured as the RSPAN VLAN and at the destination switch, the source is configured as the RSPAN VLAN.

Note

The source and destination cannot be configured as remote on the same device.

The reflector-port is configured at the source switch along with the destination RSPAN VLAN. The reflector-port forwards the mirrored traffic towards the destination switch.

Note
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.

The port mirroring commands add a mirrored port (source port) to a session identified with session-id. The session-id parameter is an integer value used to identify the session. The maximum number of sessions which can be configured is L7_MIRRORING_MAX_SESSIONS. Option rx is used to monitor only ingress packets. Option tx is used to monitor only egress packets. If no option is specified, both ingress and egress packets, RX and TX, are monitored.

A VLAN can also be configured as the source to a session (all the member ports of that VLAN are monitored).

Note
If an interface participates in some VLAN and is a *LAG* member, this VLAN cannot be assigned as a source VLAN for a Monitor session. At the same time, if an interface participates in some VLAN and this VLAN is assigned as a source VLAN for a Monitor session, the interface can be assigned as a LAG member.

Remote port mirroring is configured by giving the RSPAN VLAN ID. At the source switch the destination is configured as RSPAN VLAN and at the destination switch the source is configured as RSPAN VLAN.

Note
On the intermediate switch: RSPAN VLAN should be created, the ports connected towards Source and Destination switch should have the RSPAN VLAN participation. RSPAN VLAN egress tagging should be enabled on the interface on the intermediate switch connected towards the Destination switch.

Default	None
Format	`monitor session` *`session-id`* `destination {interface` *`unit/slot/port`* `|remote vlan` *`vlan-id`* `reflector-port` *`unit/slot/port`*`}`
Mode	Global Config

no monitor session destination

This command removes the specified probe port from the selected port mirroring session.

Format	`no monitor session` *`session-id`* `destination {interface` *`unit/slot/port`* `|remote vlan` *`vlan-id`* `reflector-port` *`unit/slot/port`*`}`
Mode	Global Config

monitor session filter

This command attaches an IP/MAC *ACL (Access Control List)* to a selected monitor session. This command configures a probe port and a monitored port for monitor session (port monitoring).

An IP/MAC ACL can be attached to a session by giving the access list number/name.

Use the filter parameter to filter a specified access group either by IP address or MAC address.

The port mirroring commands add a mirrored port (source port) to a session identified with session-id. The session-id parameter is an integer value used to identify the session. The maximum number of sessions which can be configured is L7_MIRRORING_MAX_SESSIONS.

Remote port mirroring is configured by giving the RSPAN VLAN ID. At the source switch the destination is configured as RSPAN VLAN and at the destination switch the source is configured as RSPAN VLAN.

Note
Source and destination cannot be configured as remote on the same device.

Note
IP/MAC ACL can be attached to a session by giving the access list number/name. On the platforms that do not support both IP and MAC ACLs to be assigned on the same Monitor session, an error message is thrown when user tries to configure ACLs of both types.

Default	None
Format	`monitor session` *`session-id`* `filter {ip access-group` *`acl-id/ aclname`* `| mac access-group` *`acl-name`*`}`
Mode	Global Config

no monitor session filter

This command removes the specified IP/MAC *ACL* from the selected monitoring session.

Format	`no smonitor session` *`session-id`* `filter {ip access-group | mac access-group }`
Mode	Global Config

monitor session mode

This command enables the selected port mirroring session. This command configures a probe port and a monitored port for monitor session (port monitoring).

A VLAN can be configured as the source to a session (all member ports of that VLAN are monitored). Remote port mirroring is configured by adding the RSPAN VLAN ID. At the source switch, the

destination is configured as the RSPAN VLAN and at the destination switch, the source is configured as the RSPAN VLAN.

Note
The source and destination cannot be configured as remote on the same device.

The port mirroring commands add a mirrored port (source port) to a session identified with session-id. The session-id parameter is an integer value used to identify the session. The maximum number of sessions which can be configured is L7_MIRRORING_MAX_SESSIONS. Option rx is used to monitor only ingress packets. Option tx is used to monitor only egress packets. If no option is specified, both ingress and egress packets, RX and TX, are monitored.

A VLAN can also be configured as the source to a session (all the member ports of that VLAN are monitored).

Note
If an interface participates in some VLAN and is a *LAG* member, this VLAN cannot be assigned as a source VLAN for a Monitor session. At the same time, if an interface participates in some VLAN and this VLAN is assigned as a source VLAN for a Monitor session, the interface can be assigned as a LAG member.

Remote port mirroring is configured by giving the RSPAN VLAN ID. At the source switch the destination is configured as RSPAN VLAN and at the destination switch the source is configured as RSPAN VLAN.

Note
Source and destination cannot be configured as remote on the same device.

Note
On the intermediate switch: RSPAN VLAN should be created, the ports connected towards the Source and Destination switch should have the RSPAN VLAN participation. RSPAN VLAN egress tagging should be enabled on interface on intermediate switch connected towards Destination switch.

Default	None
Format	`monitor session` *`session-id`* `mode`
Mode	Global Config

no monitor session mode

This command disables the selected port mirroring session.

Format	`no monitor session` *`session-id`* `mode`
Mode	Global Config

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

Format	`no monitor session session-id {source {interface unit/slot/port | cpu | lag} |vlan| remote vlan} | destination { interface | remote vlan | mode |filter {ip access-group | mac access-group}}]`
Mode	Global Config

no monitor

This command removes all the source ports and a destination port and restores the default value for mirroring session mode for all the configured sessions.

Note
This is a stand-alone “no” command. This command does not have a “normal” form.

Default	enabled
Format	`no monitor`
Mode	Global Config

show monitor session

This command displays the Port monitoring information for a particular mirroring session.

Note
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 1.

Format	`show monitor session session-id`
Mode	Privileged EXEC

Term	Definition
Session ID	An integer value used to identify the session. Its value can be anything between 1 and the maximum number of mirroring sessions allowed on the platform.
Admin Mode	Whether the Port Mirroring feature is enabled or disabled for the session identified with *session-id*. The possible values are Enabled and Disabled.

Term	Definition
Probe Port	Probe port (destination port) for the session identified with *session-id*. If probe port is not set then this field is blank.
Src VLAN	All member ports of this VLAN are mirrored. If the source VLAN is not configured, this field is blank.
Mirrored Port	The port that is configured as a mirrored port (source port) for the session identified with *session-id*. If no source port is configured for the session, this field is blank.
Ref. Port	This port carries all the mirrored traffic at the source switch.
Src RVLAN	The source VLAN is configured at the destination switch. If the remote VLAN is not configured, this field is blank.
Dst RVLAN	The destination VLAN is configured at the source switch. If the remote VLAN is not configured, 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.
IP *ACL*	The IP access-list id or name attached to the port mirroring session.
MAC ACL	The MAC access-list name attached to the port mirroring session.

Example 1:

```
(Extreme 220) #show monitor session 1
```

Session ID	Admin Mode	Probe Port	Src VLAN	Mirrored Port	Ref Port	Src RVLAN	Dst RVLAN	Type	IP ACL	MAC ACL
1	Enable	1/0/8		1/0/10				Rx,Tx		

Session ID	Admin Mode	Probe Port	Mirrored Port	Type
1	Enable	1/0/8	1/0/10	Rx,Tx

```
Example 2:
(Extreme 220) #show monitor session all
```

Session ID	Admin Mode	Probe Port	Src VLAN	Mirrored Port	Ref Port	Src RVLAN	Dst RVLAN	Type	IP ACL	MAC ACL
1	Enable	1/0/8		1/0/10				Rx,Tx		
2	Disable		6		0/4		10		4	

3	Disable	1/0/11		10		101
4	Enable	1/0/11	1/0/7		Tx	

Session ID	Admin Mode	Probe Port	Mirrored Port	Type
1	Enable	1/0/8	1/0/10	Rx,Tx
2	Disable			
3	Disable	1/0/11		
4	Enable	1/0/11	1/0/7	Tx

Example 3:

```
(Extreme 220) #show monitor session all
```

Session ID	Admin Mode	Probe Port	Src VLAN	Mirrored Port	Ref Port	Src RVLAN	Dst RVLAN	Type	IP ACL	MAC ACL
1	Enable	1/0/8		1/0/10				Rx		
2	Enable		6					Rx	4	
3	Disable		10					Tx		101
4	Disable	1/0/11		1/0/7				Tx		

Session ID	Admin Mode	Probe Port	Mirrored Port	Type
1	Enable	1/0/8	1/0/10	Rx
2	Enable			Rx
3	Disable			Tx
4	Disable	1/0/11	1/0/7	Tx

Example 4:

```
(Extreme 220) #show monitor session all
```

Session ID	Admin Mode	Probe Port	Src VLAN	Mirrored Port	Ref Port	Src RVLAN	Dst RVLAN	Type	IP ACL	MAC ACL
1	Enable			1/0/15	1/0/4		11	Tx	4	
2	Enable	1/0/3		1/0/15				Tx		
3	Enable			1/0/15	1/0/20		10	Rx		
4	Enable	1/0/11		1/0/15				Rx		10

Session ID	Admin Mode	Probe Port	Mirrored Port	Type
1	Enable		1/0/15	Tx
2	Enable	1/0/3	1/0/15	Tx
3	Enable		1/0/15	Rx
4	Enable	1/0/11	1/0/15	Rx

Example 5:

```
(Extreme 220) #show monitor session all
```

Session ID	Admin Mode	Probe Port	Src VLAN	Mirrored Port	Ref Port	Src RVLAN	Dst RVLAN	Type	IP ACL	MAC ACL
1	Disable									
2	Disable									
3	Enable	1/0/16	3							
4	Enable	1/0/11		1/0/16				Rx,Tx		10

Session ID	Admin Mode	Probe Port	Mirrored Port	Type
1	Disable			
2	Disable			
3	Enable	1/0/16		
4	Enable	1/0/11	1/0/16	Rx,Tx

Example 6:

```
(Extreme 220) #show monitor session all
```

Session ID	Admin Mode	Probe Port	Src VLAN	Mirrored Port	Ref Port	Src RVLAN	Dst RVLAN	Type	IP ACL	MAC ACL
1	Enable		1		1/0/4		15		4	
2	Enable	1/0/15	2							
3	Enable		3		1/0/20		10			
4	Enable	1/0/11		1/0/16				Rx,Tx		10

Session ID	Admin Mode	Probe Port	Mirrored Port	Type
1	Enable			
2	Enable	1/0/15		
3	Enable			
4	Enable	1/0/11	1/0/16	Rx,Tx

show vlan remote-span

This command displays the configured RSPAN VLAN.

Format	`show vlan remote-span`
Mode	Privileged EXEC Mode

The following example shows output for the command.

```
(Extreme 220) # show vlan remote-span
Remote SPAN VLAN
-------------------------------------------------------------------------
100,102,201,303
```

Static MAC Filtering Commands

The commands in this section describe how to configure static MAC filtering. Static MAC filtering allows you to configure destination ports for a static multicast MAC filter irrespective of the platform.

macfilter

This command adds a static MAC filter entry for the MAC address macaddr on the VLAN vlanid. The value of the macaddr parameter is a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6. The restricted MAC Addresses are: 00:00:00:00:00:00, 01:80:C2:00:00:00 to 01:80:C2:00:00:0F, 01:80:C2:00:00:20 to 01:80:C2:00:00:21, and FF:FF:FF:FF:FF:FF. The vlanid parameter must identify a valid VLAN.

The number of static mac filters supported on the system is different for MAC filters where source ports are configured and MAC filters where destination ports are configured.

You can configure the following combinations:

- Unicast MAC and source port
- Multicast MAC and source port
- Multicast MAC and destination port (only)
- Multicast MAC and source ports and destination ports

Format	`macfilter` *`macaddr vlanid`*
Mode	Global Config

no macfilter

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

The vlanid parameter must identify a valid VLAN.

Format	`no macfilter` *`macaddr vlanid`*
Mode	Global Config

macfilter adddest

Use this command to add the interface or range of interfaces to the destination filter set for the MAC filter with the given macaddr and VLAN of vlanid. The macaddr parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6. The vlanid parameter must identify a valid VLAN.

Note
Configuring a destination port list is only valid for multicast MAC addresses.

Format	`macfilter adddest` *`macaddr`*
Mode	Interface Config

no macfilter adddest

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

Format	`no macfilter adddest` *`macaddr`*
Mode	Interface Config

macfilter adddest all

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

Note
Configuring a destination port list is only valid for multicast MAC addresses.

Format	`macfilter adddest all` *`macaddr`*
Mode	Global Config

no macfilter adddest all

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

Format	`no macfilter adddest all` *`macaddr`*
Mode	Global Config

macfilter addsrc

This command adds the interface or range of interfaces to the source filter set for the MAC filter with the MAC address of macaddr and VLAN of vlanid. The macaddr parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6. The vlanid parameter must identify a valid VLAN.

Format	`macfilter addsrc` *`macaddr vlanid`*
Mode	Interface Config

no macfilter addsrc

This command removes a port from the source filter set for the MAC filter with the MAC address of macaddr and VLAN of vlanid. The macaddr parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6. The vlanid parameter must identify a valid VLAN.

Format	`no macfilter addsrc` *`macaddr vlanid`*
Mode	Interface Config

macfilter addsrc all

This command adds all interfaces to the source filter set for the MAC filter with the MAC address of macaddr and vlanid. You must specify the macaddr parameter as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6. The vlanid parameter must identify a valid VLAN.

Format	`macfilter addsrc all` *`macaddr vlanid`*
Mode	Global Config

no macfilter addsrc all

This command removes all interfaces to the source filter set for the MAC filter with the MAC address of macaddr and VLAN of vlanid. You must specify the macaddr parameter as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6.

The vlanid parameter must identify a valid VLAN.

Format	`no macfilter addsrc all` *`macaddr vlanid`*
Mode	Global Config

show mac-address-table static

This command displays the Static MAC Filtering information for all Static MAC Filters. If you specify all, all the Static MAC Filters in the system are displayed. If you supply a value for macaddr, you must also enter a value for vlanid, and the system displays Static MAC Filter information only for that MAC address and VLAN.

Format	`show mac-address-table static {`*`macaddr vlanid`*` | all}`
Mode	Privileged EXEC

Column	Meaning
MAC Address	The MAC Address of the static MAC filter entry.
VLAN ID	The VLAN ID of the static MAC filter entry.
Source Port(s)	The source port filter set's slot and port(s).

Note
Only multicast address filters will have destination port lists.

show mac-address-table staticfiltering

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

Format	`show mac-address-table staticfiltering`
Mode	Privileged EXEC

Column	Meaning
VLAN ID	The VLAN in which the MAC Address is learned.
MAC Address	A unicast MAC address for which the switch has forwarding and or filtering information. As the data is gleaned from the MFDB, the address will be a multicast address. The format is 6 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB.
Type	The type of the entry. Static entries are those that are configured by the end user. Dynamic entries are added to the table as a result of a learning process or protocol.
Description	The text description of this multicast table entry.
Interfaces	The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).

DHCP L2 Relay Agent Commands

You can enable the switch to operate as a *DHCP (Dynamic Host Configuration Protocol)* Layer 2 relay agent to relay DHCP requests from clients to a Layer 3 relay agent or server. The Circuit ID and Remote ID can be added to DHCP requests relayed from clients to a DHCP server. This information is included in DHCP Option 82, as specified in sections 3.1 and 3.2 of RFC3046.

dhcp l2relay

This command enables the *DHCP* Layer 2 Relay agent for an interface a range of interfaces in, or all interfaces. The subsequent commands mentioned in this section can only be used when the DHCP L2 relay is enabled.

Format	`dhcp l2relay`
Mode	• Global Config • Interface Config

no dhcp l2relay

This command disables *DHCP* Layer 2 relay agent for an interface or range of interfaces.

Format	`no dhcp l2relay`
Mode	• Global Config • Interface Config

dhcp l2relay circuit-id subscription

This command sets the Option-82 Circuit ID for a given service subscription identified by subscription-string on a given interface. The subscription-string is a character string which needs to be matched with a configured DOT1AD subscription string for correct operation. When circuit-id is enabled using this command, all Client *DHCP* requests that fall under this service subscription are added with Option-82 circuit-id as the incoming interface number.

Default	Disabled
Format	`dhcp l2relay circuit-id subscription` *`subscription-string`*
Mode	Interface Config

no dhcp l2relay circuit-id subscription

This command resets the Option-82 Circuit ID for a given service subscription identified by subscription-string on a given interface. The subscription-string is a character string which needs to be matched with a configured DOT1AD subscription string for correct operation. When circuit-id is disabled using this command, all Client *DHCP* requests that fall under this service subscription are no longer added with Option-82 circuit-id.

Format	`no dhcp l2relay circuit-id subscription` *`subscription-string`*
Mode	Interface Config

dhcp l2relay circuit-id vlan

This parameter sets the *DHCP* Option-82 Circuit ID for a VLAN. When enabled, the interface number is added as the Circuit ID in DHCP option 82.

Format	`dhcp l2relay circuit-id vlan` *`vlan-list`*
Mode	Global Config

Parameter	Description
`vlan-list`	The VLAN ID. The range is 1–4093. Separate nonconsecutive IDs with a comma (,) no spaces and no zeros in between the range. Use a dash (-) for the range.

no dhcp l2relay circuit-id vlan

This parameter clears the *DHCP* Option-82 Circuit ID for a VLAN.

Format	`no dhcp l2relay circuit-id vlan` *`vlan-list`*
Mode	Global Config

dhcp l2relay remote-id subscription

This command sets the Option-82 Remote-ID string for a given service subscription identified by subscription-string on a given interface or range of interfaces. The subscription-string is a character string which needs to be matched with a configured DOT1AD subscription string for correct operation. The remoteid-string is a character string. When remote-id string is set using this command, all Client *DHCP* requests that fall under this service subscription are added with Option-82 Remote-id as the configured remote-id string.

Default	empty string
Format	`dhcp l2relay remote-id` *`remoteid-string`* `subscription-name` *`subscription-string`*
Mode	Interface Config

no dhcp l2relay remote-id subscription

This command resets the Option-82 Remote-ID string for a given service subscription identified by subscription-string on a given interface. The subscription-string is a character string which needs to be matched with a configured DOT1AD subscription string for correct operation. When remote-id string is reset using this command, the Client *DHCP* requests that fall under this service subscription are not added with Option-82 Remote-id.

Format	`no dhcp l2relay remote-id` *`remoteid-string`* `subscription-name` *`subscription-string`*
Mode	Interface Config

dhcp l2relay remote-id vlan

This parameter sets the *DHCP* Option-82 Remote ID for a VLAN and subscribed service (based on subscription-name).

Format	`dhcp l2relay remote-id` *`remote-id-string`* `vlan` *`vlan-list`*
Mode	Global Config

Parameter	Description
`vlan-list`	The VLAN ID. The range is 1–4093. Separate nonconsecutive IDs with a comma (,) no spaces and no zeros in between the range. Use a dash (–) for the range.

no dhcp l2relay remote-id vlan

This parameter clears the *DHCP* Option-82 Remote ID for a VLAN and subscribed service (based on subscription-name).

Format	`no dhcp l2relay remote-id vlan` *`vlan-list`*
Mode	Global Config

dhcp l2relay 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	Disabled
Format	`dhcp l2relay vlan vlan-list`
Mode	Global Config

Parameter	Description
vlan-list	The VLAN ID. The range is 1–4093. Separate nonconsecutive IDs with a comma (,) no spaces and no zeros in between the range. Use a dash (–) for the range.

no dhcp l2relay vlan

Use this command to disable the *DHCP* L2 Relay agent for a set of VLANs.

Format	`no dhcp l2relay vlan vlan-list`
Mode	Global Config

show dhcp l2relay all

This command displays the summary of DHCP L2 Relay configuration.

Format	`show dhcp l2relay all`
Mode	Privileged EXEC

The following example shows CLI display output for the command.

```
(Extreme 220) (Switching) #show dhcp l2relay all
DHCP L2 Relay is Enabled.
Interface  L2RelayMode   TrustMode
---------  -----------  --------------
 0/2        Enabled      untrusted
 0/4        Disabled     trusted
VLAN Id    L2 Relay  CircuitId  RemoteId
-------- ----------  ----------- ------------
 3          Disabled    Enabled    --NULL--
5          Enabled     Enabled    --NULL--
 6          Enabled     Enabled    extreme
 7          Enabled     Disabled   --NULL--
 8          Enabled     Disabled   --NULL--
 9          Enabled     Disabled   --NULL--
 10         Enabled     Disabled   --NULL--
```

show dhcp l2relay circuit-id vlan

This command displays *DHCP* circuit-id vlan configuration.

Format	show dhcp l2relay circuit-id vlan *vlan-list*
Mode	Privileged EXEC

Parameter	Description
vlan-list	Enter VLAN IDs in the range 1–4093. Use a dash (-) to specify a range or a comma (,) to separate VLAN IDs in a list. Spaces and zeros are not permitted.

show dhcp l2relay interface

This command displays DHCP L2 relay configuration specific to interfaces.

Format	show dhcp l2relay interface {all | *interface-num*}
Mode	Privileged EXEC

The following example shows CLI display output for the command.

```
(Extreme 220) (Switching) #show dhcp l2relay interface all
DHCP L2 Relay is  Enabled.
Interface  L2RelayMode   TrustMode
---------  -----------  --------------
 0/2        Enabled      untrusted
 0/4        Disabled     trusted
```

show dhcp l2relay remote-id vlan

This command displays DHCP Remote-id vlan configuration.

Format	show dhcp l2relay remote-id vlan *vlan-list*
Mode	Privileged EXEC

Parameter	Description
vlan-list	Enter VLAN IDs in the range 1–4093. Use a dash (-) to specify a range or a comma (,) to separate VLAN IDs in a list. Spaces and zeros are not permitted.

show dhcp l2relay stats interface

This command displays statistics specific to DHCP L2 Relay configured interface.

Format	show dhcp l2relay stats interface {all | *interface-num*}
Mode	Privileged EXEC

The following example shows CLI display output for the command.

```
(Extreme 220) (Switching) #show dhcp l2relay stats interface all
DHCP L2 Relay is  Enabled.
Interface  UntrustedServer    UntrustedClient  TrustedServer     TrustedClient
```

```
                MsgsWithOpt82        MsgsWithOpt82        MsgsWithoutOpt82
MsgsWithoutOpt82
---------  --------------- -----------------  ----------------- --------------
 0/1                 0                    0                   0                  0
 0/2               0                    0                   3                  7
 0/3               0                    0                   0                  0
 0/4               0                    12                  0                  0
 0/5               0                    0                   0                  0
 0/6               3                    0                   0                    0
 0/7               0                    0                   0                  0
 0/8               0                    0                   0                  0
 0/9                  0                       0
0                      0
```

show dhcp l2relay agent-option vlan

This command displays the DHCP L2 Relay Option-82 configuration specific to VLAN.

Format	`show dhcp l2relay agent-option vlan` *`vlan-range`*
Mode	Privileged EXEC

The following example shows CLI display output for the command.

```
(Extreme 220) (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    extreme
7           Enabled     Disabled   --NULL--
8           Enabled     Disabled   --NULL--
9           Enabled     Disabled   --NULL--
10          Enabled     Disabled   --NULL--
```

show dhcp l2relay vlan

This command displays DHCP vlan configuration.

Format	`show dhcp l2relay vlan` *`vlan-list`*
Mode	Privileged EXEC

Parameter	Description
`vlan-list`	Enter VLAN IDs in the range 1–4093. Use a dash (-) to specify a range or a comma (,) to separate VLAN IDs in a list. Spaces and zeros are not permitted.

clear dhcp l2relay statistics interface

Use this command to reset the *DHCP* L2 relay counters to zero. Specify the port with the counters to clear, or use the **`all`** keyword to clear the counters on all ports.

Format	`clear dhcp l2relay statistics interface {`*`unit/slot/port`* `| all}`
Mode	Privileged EXEC

DHCP Client Commands

200 Series can include vendor and configuration information in *DHCP* client requests relayed to a DHCP server. This information is included in DHCP Option 60, Vendor Class Identifier. The information is a string of 128 octets.

dhcp client vendor-id-option

This command enables the inclusion of *DHCP* Option-60, Vendor Class Identifier included in the requests transmitted to the DHCP server by the DHCP client operating in the 200 Series switch.

Note
This feature is available for 220 switches only.

Format	`dhcp client vendor-id-option` *`string`*
Mode	Global Config

no dhcp client vendor-id-option

This command disables the inclusion of DHCP Option-60, Vendor Class Identifier included in the requests transmitted to the *DHCP* server by the DHCP client operating in the 200 Series switch.

Format	`no dhcp client vendor-id-option`
Mode	Global Config

dhcp client vendor-id-option-string

This parameter sets the *DHCP* Vendor Option-60 string to be included in the requests transmitted to the DHCP server by the DHCP client operating in the 200 Series switch.

Note
This feature is available for 220 switches only.

Format	`dhcp client vendor-id-option-string` *`string`*
Mode	Global Config

no dhcp client vendor-id-option-string

This parameter clears the *DHCP* Vendor Option-60 string.

Format	`no dhcp client vendor-id-option-string`
Mode	Global Config

show dhcp client vendor-id-option

This command displays the configured administration mode of the vendor-id-option and the vendor-id string to be included in Option-43 in *DHCP* requests.

Note
This feature is available for 220 switches only.

Format	`show dhcp client vendor-id-option`
Mode	Privileged EXEC

The following example shows CLI display output for the command.

```
(Extreme 220) #show dhcp client vendor-id-option
DHCP Client Vendor Identifier Option is Enabled
DHCP Client Vendor Identifier Option string is FastpathClient.
```

DHCP Snooping Configuration Commands

This section describes commands used to configure *DHCP* Snooping.

ip dhcp snooping

Use this command to enable *DHCP* Snooping globally.

Default	Disabled
Format	`ip dhcp snooping`
Mode	Global Config

no ip dhcp snooping

Use this command to disable *DHCP* Snooping globally.

Format	`no ip dhcp snooping`
Mode	Global Config

ip dhcp snooping vlan

Use this command to enable *DHCP* Snooping on a list of comma-separated VLAN ranges.

Default	Disabled
Format	`ip dhcp snooping vlan vlan-list`
Mode	Global Config

no ip dhcp snooping vlan

Use this command to disable *DHCP* Snooping on VLANs.

Format	`no ip dhcp snooping vlan vlan-list`
Mode	Global Config

ip dhcp snooping verify mac-address

Use this command to enable verification of the source MAC address with the client hardware address in the received DCHP message.

Default	Enabled
Format	`ip dhcp snooping verify mac-address`
Mode	Global Config

no ip dhcp snooping verify mac-address

Use this command to disable verification of the source MAC address with the client hardware address.

Format	`no ip dhcp snooping verify mac-address`
Mode	Global Config

ip dhcp snooping database

Use this command to configure the persistent location of the *DHCP* Snooping database. This can be local or a remote file on a given IP machine.

Default	local
Format	`ip dhcp snooping database {local | tftp://hostIP/filename}`
Mode	Global Config

ip dhcp snooping database write-delay

Use this command to configure the interval in seconds at which the *DHCP* Snooping database will be persisted. The interval value ranges from 15 to 86400 seconds.

Default	300 seconds
Format	`ip dhcp snooping database write-delay` *`seconds`*
Mode	Global Config

no ip dhcp snooping database write-delay

Use this command to set the write delay value to the default value.

Format	`no ip dhcp snooping database write-delay`
Mode	Global Config

ip dhcp snooping binding

Use this command to configure static *DHCP* Snooping binding.

Format	`ip dhcp snooping binding` *`mac-address`* **`vlan`** *`vlan id ip address`* **`interface`** *`interface id`*
Mode	Global Config

no ip dhcp snooping binding

Use this command to remove the *DHCP* static entry from the DHCP Snooping database.

Format	`no ip dhcp snooping binding` *`mac-address`*
Mode	Global Config

ip dhcp filtering trust

Use this command to enable trusted mode on the interface if the previously saved configuration or applied script contains this command.

Format	`ip dhcp filtering trust` *`interface id`*
Mode	Global Config

no ip dhcp filtering trust

Use this command to disable trusted mode on the interface.

Format	`no ip dhcp filtering trust` *`interface id`*
Mode	Global Config

ip verify binding

Use this command to configure static IP source guard (IPSG) entries.

Format	`ip verify binding` *`mac-address`* `vlan` *`vlan id ip address interface interface id`*
Mode	Global Config

no ip verify binding

Use this command to remove the IPSG static entry from the IPSG database.

Format	`no ip verify binding` *`mac-address`* `vlan` *`vlan id ip address interface interface id`*
Mode	Global Config

ip dhcp snooping limit

Use this command to control the rate at which the *DHCP* Snooping messages come on an interface or range of interfaces. By default, rate limiting is disabled. When enabled, the rate can range from 0 to 300 packets per second. The burst level range is 1 to 15 seconds.

Default	Disabled (no limit)
Format	`ip dhcp snooping limit {rate pps [`*`burst interval seconds`*`]}`
Mode	Interface Config

no ip dhcp snooping limit

Use this command to set the rate at which the *DHCP* Snooping messages come, and the burst level, to the defaults.

Format	`no ip dhcp snooping limit`
Mode	Interface Config

ip dhcp snooping log-invalid

Use this command to control the logging *DHCP* messages filtration by the DHCP Snooping application. This command can be used to configure a single interface or a range of interfaces.

Default	Disabled
Format	`ip dhcp snooping log-invalid`
Mode	Interface Config

no ip dhcp snooping log-invalid

Use this command to disable the logging *DHCP* messages filtration by the DHCP Snooping application.

Format	`no ip dhcp snooping log-invalid`
Mode	Interface Config

ip dhcp snooping trust

Use this command to configure an interface or range of interfaces as trusted.

Default	Disabled
Format	`ip dhcp snooping trust`
Mode	Interface Config

no ip dhcp snooping trust

Use this command to configure the port as untrusted.

Format	`no ip dhcp snooping trust`
Mode	Interface Config

ip verify source

Use this command to configure the IPSG source ID attribute to filter the data traffic in the hardware. Source ID is the combination of IP address and MAC address. Normal command allows data traffic filtration based on the IP address. With the “port-security” option, the data traffic will be filtered based on the IP and MAC addresses.

This command can be used to configure a single interface or a range of interfaces.

Default	the source ID is the IP address
Format	`ip verify source {port-security}`
Mode	Interface Config

no ip verify source

Use this command to disable the IPSG configuration in the hardware. You cannot disable port-security alone if it is configured.

Format	`no ip verify source`
Mode	Interface Config

show ip dhcp snooping

Use this command to display the *DHCP* Snooping global configurations and per port configurations.

Format	`show ip dhcp snooping`
Mode	• Privileged EXEC • User EXEC

Column	Meaning
Interface	The interface for which data is displayed.
Trusted	If it is enabled, DHCP snooping considers the port as trusted. The factory default is disabled.
Log Invalid Pkts	If it is enabled, DHCP snooping application logs invalid packets on the specified interface.

The following example shows CLI display output for the command.

```
(Extreme 220) #show ip dhcp snooping
DHCP snooping is Disabled
DHCP snooping source MAC verification is enabled
DHCP snooping is enabled on the following VLANs:
11 - 30, 40
Interface   Trusted    Log Invalid Pkts
---------   --------   ----------------
0/1          Yes             No
0/2          No             Yes
0/3          No             Yes
0/4          No              No
0/6          No              No
```

show ip dhcp snooping binding

Use this command to display the *DHCP* Snooping binding entries. To restrict the output, use the following options:

- Dynamic: Restrict the output based on DCHP snooping.
- Interface: Restrict the output based on a specific interface.
- Static: Restrict the output based on static entries.
- VLAN: Restrict the output based on VLAN.

Format	`show ip dhcp snooping binding [{static/dynamic}] [`**`interface`** *`unit/slot/port`*`] [`*`vlan id`*`]`
Mode	• Privileged EXEC • User EXEC

Column	Meaning
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.

Column	Meaning
Type	Binding type; statically configured from the CLI or dynamically learned.
Lease (sec)	The remaining lease time for the entry.

The following example shows CLI display output for the command.

```
(Extreme 220) #show ip dhcp snooping binding
Total number of bindings: 2
MAC Address          IP Address   VLAN  Interface  Type
Lease time (Secs)
------------------  ------------  ----  ---------  ----            ------------------
00:02:B3:06:60:80   210.1.1.3      10
0/1                                                                        86400
00:0F:FE:00:13:04   210.1.1.4      10
0/1                                                                          86400
```

show ip dhcp snooping database

Use this command to display the *DHCP* Snooping configuration related to the database persistence.

Format	`show ip dhcp snooping database`
Mode	• Privileged EXEC • User EXEC

Column	Meaning
Agent URL	Bindings database agent URL.
Write Delay	The maximum write time to write the database into local or remote.

The following example shows CLI display output for the command.

```
(Extreme 220) #show ip dhcp snooping database
agent url:  /10.131.13.79:/sai1.txt
write-delay:  5000
```

show ip dhcp snooping interfaces

Use this command to show the *DHCP* Snooping status of the interfaces.

Format	`show ip dhcp snooping interfaces`
Mode	Privileged EXEC

The following example shows CLI display output for the command.

```
(Extreme 220) #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
```

```
(Extreme 220) #show ip dhcp snooping interfaces ethernet 1/g15
 Interface    Trust State                                Rate Limit                Burst
Interval
                                          (pps)             (seconds)
-----------   ----------   ----------   --------------
    1/g15                    Yes               15                    1
```

show ip dhcp snooping statistics

Use this command to list statistics for *DHCP* Snooping security violations on untrusted ports.

Format	`show ip dhcp snooping statistics`
Mode	• Privileged EXEC • User EXEC

Column	Meaning
Interface	The IP address of the interface in *`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 Ifc Mismatch	Represents the number of DHCP release and Deny messages received on the different ports than learned previously.
DHCP Server Msgs Rec'd	Represents the number of DHCP server messages received on Untrusted ports.

The following example shows CLI display output for the command.

```
(Extreme 220) #show ip dhcp snooping statistics
 Interface    MAC Verify   Client Ifc   DHCP Server
               Failures     Mismatch    Msgs Rec'd
-----------   ----------   ----------   -----------
1/0/2                  0            0             0
1/0/3                  0            0             0
1/0/4                  0            0             0
1/0/5                  0            0             0
1/0/6                  0            0             0
1/0/7                  0            0             0
1/0/8                  0            0             0
1/0/9                  0            0             0
1/0/10                 0            0             0
1/0/11                 0            0             0
1/0/12                 0            0             0
1/0/13                 0            0             0
1/0/14                 0            0             0
1/0/15                 0            0             0
1/0/16                 0            0             0
1/0/17                 0            0             0
1/0/18                 0            0             0
1/0/19                 0            0             0
1/0/20                 0            0             0
```

clear ip dhcp snooping binding

Use this command to clear all *DHCP* Snooping bindings on all interfaces or on a specific interface.

Format	`clear ip dhcp snooping binding [interface` *`unit/slot/port`*`]`
Mode	• Privileged EXEC • User EXEC

clear ip dhcp snooping statistics

Use this command to clear all *DHCP* Snooping statistics.

Format	`clear ip dhcp snooping statistics`
Mode	• Privileged EXEC • User EXEC

show ip verify source

Use this command to display the IPSG configurations on all ports.

Format	`show ip verify source`
Mode	• Privileged EXEC • User EXEC

Column	Meaning
Interface	Interface address in *`unit/slot/port`* format.
Filter Type	Is one of two values: • ip-mac: User has configured MAC address filtering on this interface. • ip: Only IP address filtering on this interface.
IP Address	IP address of the interface
MAC Address	If MAC address filtering is not configured on the interface, the MAC Address field is empty. If port security is disabled on the interface, then the MAC Address field displays “permit-all.”
VLAN	The VLAN for the binding rule.

The following example shows CLI display output for the command.

```
(Extreme 220) #show ip verify source
Interface  Filter Type    IP Address       MAC Address      Vlan
---------  -----------  ---------------  -----------------  -----
    0/1     ip-mac       210.1.1.3       00:02:B3:06:60:80     10
    0/1     ip-mac       210.1.1.4       00:0F:FE:00:13:04     10
```

show ip verify interface

Use this command to display the IPSG filter type for a specific interface.

Format	`show ip verify interface unit/slot/port`
Mode	• Privileged EXEC • User EXEC

Column	Meaning
Interface	Interface address in *`unit/slot/port`* format.
Filter Type	Is one of two values: • ip-mac: User has configured MAC address filtering on this interface. • ip: Only IP address filtering on this interface.

show ip source binding

Use this command to display the IPSG bindings.

Format	`show ip source binding [{dhcp-snooping|static}] [interface` *`unit/slot/port`*`] [vlan id]`
Mode	• Privileged EXEC • User EXEC

Column	Meaning
MAC Address	The MAC address for the entry that is added.
IP Address	The IP address of the entry that is added.
Type	Entry type; statically configured from CLI or dynamically learned from *DHCP* Snooping.
VLAN	VLAN for the entry.
Interface	IP address of the interface in *`unit/slot/port`* format.

The following example shows CLI display output for the command.

```
(Extreme 220) #show ip source binding
MAC Address       IP Address       Type         Vlan     Interface
----------------  ---------------  -------------  -----  -------------
00:00:00:00:00:08          1.2.3.4  dhcp-snooping     2        1/0/1
00:00:00:00:00:09          1.2.3.4  dhcp-snooping     3        1/0/1
00:00:00:00:00:0A          1.2.3.4  dhcp-snooping     4        1/0/1
```

IGMP Snooping Configuration Commands

This section describes the commands used to configure *IGMP* snooping. 200 Series software supports IGMP Versions 1, 2, and 3. The IGMP snooping feature can help conserve bandwidth because it allows

the switch to forward IP multicast traffic only to connected hosts that request multicast traffic. IGMPv3 adds source filtering capabilities to IGMP versions 1 and 2.

Note

This note clarifies the prioritization of MGMD Snooping Configurations. Many of the IGMP/MLD Snooping commands are available both in the Interface and VLAN modes. Operationally the system chooses or prefers the VLAN configured values over the Interface configured values for most configurations when the interface participates in the VLAN.

set igmp

This command enables *IGMP* Snooping on the system (Global Config Mode), an interface, or a range of interfaces. This command also enables IGMP snooping on a particular VLAN (VLAN Config Mode) and can enable IGMP snooping on all interfaces participating in a VLAN.

If an interface has IGMP Snooping enabled and you enable this interface for routing or enlist it as a member of a port-channel (*LAG*), IGMP Snooping functionality is disabled on that interface. IGMP Snooping functionality is re-enabled if you disable routing or remove port-channel (LAG) membership from an interface that has IGMP Snooping enabled.

The IGMP application supports the following activities:

- Validation of the IP header checksum (as well as the IGMP header checksum) and discarding of the frame upon checksum error.
- Maintenance of the forwarding table entries based on the MAC address versus the IP address.
- Flooding of unregistered multicast data packets to all ports in the VLAN.

Default	Disabled
Format	`set igmp [vlan_id]`
Mode	• Global Config • Interface Config • VLAN Config

no set igmp

This command disables *IGMP* Snooping on the system, an interface, a range of interfaces, or a VLAN.

Format	`no set igmp [vlan_id]`
Mode	• Global Config • Interface Config • VLAN Config

set igmp header-validation

This command enables header validation for *IGMP* messages.

When header validation is enabled, IGMP Snooping checks:

- The time-to-live (TTL) field in the IGMP header and drops packets where TTL is not equal to 1. The TTL field should always be set to 1 in the headers of IGMP reports and queries.
- The presence of the router alert option (9404) in the IP packet header of the IGMPv2 message and drops packets that do not include this option.
- The presence of the router alert option (9404) and ToS Byte = 0xC0 (Internet Control) in the IP packet header of IGMPv3 message and drops packets that do not include these options.

Default	Enabled
Format	`set igmp header-validation`
Mode	Global Config

no set igmp header-validation

This command disables header validation for *IGMP* messages.

Format	`no set igmp header-validation`
Mode	Global Config

set igmp interfacemode

This command enables *IGMP* Snooping on all interfaces. If an interface has IGMP Snooping enabled and you enable this interface for routing or enlist it as a member of a port-channel (*LAG*), IGMP Snooping functionality is disabled on that interface. IGMP Snooping functionality is re-enabled if you disable routing or remove port-channel (LAG) membership from an interface that has IGMP Snooping enabled.

Default	Disabled
Format	`set igmp interfacemode`
Mode	Global Config

no set igmp interfacemode

This command disables *IGMP* Snooping on all interfaces.

Format	`no set igmp interfacemode`
Mode	Global Config

set igmp fast-leave

This command enables or disables *IGMP* Snooping fast-leave admin mode on a selected interface, a range of interfaces, or a VLAN. Enabling fast-leave allows the switch to immediately remove the layer 2 LAN interface from its forwarding table entry upon receiving an IGMP leave message for that multicast group without first sending out MAC-based general queries to the interface.

You should enable fast-leave admin mode only on VLANs where only one host is connected to each layer 2 LAN port. This prevents the inadvertent dropping of the other hosts that were connected to the

same layer 2 LAN port but were still interested in receiving multicast traffic directed to that group. Also, fast-leave processing is supported only with IGMP version 2 hosts.

Default	Disabled
Format	`set igmp fast-leave [vlan_id]`
Mode	Interface Config Interface Range VLAN Config

no set igmp fast-leave

This command disables *IGMP* Snooping fast-leave admin mode on a selected interface.

Format	`no set igmp fast-leave [vlan_id]`
Mode	Interface Config Interface Range VLAN Config

set igmp groupmembership-interval

This command sets the *IGMP* Group Membership Interval time on a VLAN, one interface, a range of interfaces, or all interfaces. The Group Membership Interval time is the amount of time in seconds that a switch waits for a report from a particular group on a particular interface before deleting the interface from the entry. This value must be greater than the IGMPv3 Maximum Response time value. The range is 2 to 3600 seconds.

Default	260 seconds
Format	`set igmp groupmembership-interval [vlan_id] 2-3600`
Mode	• Interface Config • Global Config • VLAN Config

no set igmp groupmembership-interval

This command sets the IGMPv3 Group Membership Interval time to the default value.

Format	`no set igmp groupmembership-interval [vlan_id]`
Mode	• Interface Config • Global Config • VLAN Config

set igmp maxresponse

This command sets the *IGMP* Maximum Response time for the system, on a particular interface or VLAN, or on a range of interfaces. The Maximum Response time is the amount of time in seconds that a switch will wait after sending a query on an interface because it did not receive a report for a particular group in that interface. This value must be less than the IGMP Query Interval time value. The range is 1 to 25 seconds.

Default	10 seconds
Format	`set igmp maxresponse [vlan_id] 1-25`
Mode	• Global Config • Interface Config • VLAN Config

no set igmp maxresponse

This command sets the max response time (on the interface or VLAN) to the default value.

Format	`no set igmp maxresponse [vlan_id]`
Mode	• Global Config • Interface Config • VLAN Config

set igmp mcrtrexpiretime

This command sets the Multicast Router Present Expiration time. The time is set for the system, on a particular interface or VLAN, or on a range of interfaces. This is the amount of time in seconds that a switch waits for a query to be received on an interface before the interface is removed from the list of interfaces with multicast routers attached. The range is 0 to 3600 seconds. A value of 0 indicates an infinite time-out, that is, no expiration.

Default	0
Format	`set igmp mcrtrexpiretime [vlan_id] 0-3600`
Mode	• Global Config • Interface Config • VLAN Config

no set igmp mcrtrexpiretime

This command sets the Multicast Router Present Expiration time to 0. The time is set for the system, on a particular interface or a VLAN.

Format	`no set igmp mcrtrexpiretime [vlan_id]`
Mode	• Global Config • Interface Config • VLAN Config

Format	`no set igmp mcrtrexpiretime vlan_id`
Mode	VLAN Config

set igmp mrouter

This command configures the VLAN ID (vlan_id) that has the multicast router mode enabled.

Format	`set igmp mrouter vlan_id`
Mode	Interface Config

no set igmp mrouter

This command disables multicast router mode for a particular VLAN ID (vlan_id).

Format	`no set igmp mrouter vlan_id`
Mode	Interface Config

set igmp mrouter interface

This command configures the interface or range of interfaces as a multicast router interface. When configured as a multicast router interface, the interface is treated as a multicast router interface in all VLANs.

Default	Disabled
Format	`set igmp mrouter interface`
Mode	Interface Config

no set igmp mrouter interface

This command disables the status of the interface as a statically configured multicast router interface.

Format	`no set igmp mrouter interface`
Mode	Interface Config

set igmp report-suppression

Use this command to suppress the *IGMP* reports on a given VLAN ID. In order to optimize the number of reports traversing the network with no added benefits, a Report Suppression mechanism is implemented. When more than one client responds to an MGMD query for the same Multicast Group address within the max-response-time, only the first response is forwarded to the query and others are suppressed at the switch.

Default	Disabled
Format	`set igmp report-suppression vlan-id`
Mode	VLAN Config

Parameter	Description
vlan-id	A valid VLAN ID. Range is 1 to 4093.

The following shows an example of the command.

```
(Extreme 220) (Switching) #vlan database
(Extreme 220) (Switching) (Vlan)#set igmp report-suppression ?
<1-4093>                  Enter VLAN ID.
(Extreme 220) (Switching) (Vlan)#set igmp report-suppression 1
```

no set igmp report-suppression

Use this command to return the system to the default.

Format	`no set igmp report-suppression`
Mode	VLAN Config

show igmpsnooping

This command displays *IGMP* Snooping information for a given unit/slot/port or VLAN. Configured information is displayed whether IGMP Snooping is enabled.

Format	`show igmpsnooping [unit/slot/port | vlan_id]`
Mode	Privileged EXEC

When the optional arguments unit/slot/port or vlan_id are not used, the command displays the following information:

Column	Meaning
Admin Mode	Whether IGMP Snooping is active on the switch.
Multicast Control Frame Count	The number of multicast control frames that are processed by the CPU.
Interface Enabled for IGMP Snooping	The list of interfaces on which IGMP Snooping is enabled.
VLANS Enabled for IGMP Snooping	The list of VLANS on which IGMP Snooping is enabled.

When you specify the unit/slot/port values, the following information appears:

Column	Meaning
IGMP Snooping Admin Mode	Whether IGMP Snooping is active on the interface.
Fast Leave Mode	Whether IGMP Snooping Fast-leave is active on the interface.
Group Membership Interval	The amount of time in seconds that a switch will wait for a report from a particular group on a particular interface before deleting the interface from the entry. This value may be configured.
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:

Column	Meaning
VLAN ID	The VLAN ID.
IGMP Snooping Admin Mode	Whether IGMP Snooping is active on the VLAN.
Fast Leave Mode	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 Suppression Mode	Whether IGMP reports, set by the `set igmp report-suppression` command, are enabled or not. (See set igmp report-suppression on page 437.)

The following example shows CLI display output for the command.

```
(Extreme 220) (Switching) #show igmpsnooping 1
VLAN ID..................................... 1
IGMP Snooping Admin Mode..................... Disabled
Fast Leave Mode.............................. Disabled
Group Membership Interval (secs)............. 260
Max Response Time (secs)..................... 10
Multicast Router Expiry Time (secs)..... 0
Report Suppression Mode...................... Enabled
```

show igmpsnooping mrouter interface

This command displays information about statically configured ports.

Format	show igmpsnooping mrouter interface *unit/slot/port*
Mode	Privileged EXEC

Column	Meaning
Interface	The port on which multicast router information is being displayed.
Multicast Router Attached	Whether multicast router is statically enabled on the interface.
VLAN ID	The list of VLANs of which the interface is a member.

show igmpsnooping mrouter vlan

This command displays information about statically configured ports.

Format	show igmpsnooping mrouter vlan *unit/slot/port*
Mode	Privileged EXEC

Column	Meaning
Interface	The port on which multicast router information is being displayed.
VLAN ID	The list of VLANs of which the interface is a member.

show mac-address-table igmpsnooping

This command displays the *IGMP* Snooping entries in the MFDB table.

Format	show mac-address-table igmpsnooping
Mode	Privileged EXEC

Column	Meaning
VLAN ID	The VLAN in which the MAC address is learned.
MAC Address	A multicast MAC address for which the switch has forwarding or filtering information. The format is 6 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB.
Type	The type of the entry, which is either static (added by the user) or dynamic (added to the table as a result of a learning process or protocol).
Description	The text description of this multicast table entry.
Interfaces	The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).

IGMP Snooping Querier Commands

IGMP Snooping requires that one central switch or router periodically query all end-devices on the network to announce their multicast memberships. This central device is the “IGMP Querier”. The IGMP query responses, known as IGMP reports, keep the switch updated with the current multicast group membership on a port-by-port basis. If the switch does not receive updated membership information in a timely fashion, it will stop forwarding multicasts to the port where the end device is located.

This section describes commands used to configure and display information on IGMP Snooping Queriers on the network and, separately, on VLANs.

Note
This note clarifies the prioritization of MGMD Snooping Configurations. Many of the IGMP/MLD Snooping commands are available both in the Interface and VLAN modes. Operationally the system chooses or prefers the VLAN configured values over the Interface configured values for most configurations when the interface participates in the VLAN.

set igmp querier

Use this command to enable *IGMP* Snooping Querier on the system, using Global Config mode, or on a VLAN. Using this command, you can specify the IP Address that the Snooping Querier switch should use as the source address while generating periodic queries.

If a VLAN has IGMP Snooping Querier enabled and IGMP Snooping is operationally disabled on it, IGMP Snooping Querier functionality is disabled on that VLAN. IGMP Snooping functionality is re-enabled if IGMP Snooping is operational on the VLAN.

Note
The Querier IP Address assigned for a VLAN takes preference over global configuration.

The IGMP Snooping Querier application supports sending periodic general queries on the VLAN to solicit membership reports.

Default	Disabled
Format	`set igmp querier [vlan-id] [address ipv4_address]`
Mode	• Global Config • VLAN Mode

no set igmp querier

Use this command to disable *IGMP* Snooping Querier on the system. Use the optional address parameter to reset the querier address to 0.0.0.0.

Format	`no set igmp querier [vlan-id] [address]`
Mode	• Global Config • VLAN Mode

set igmp querier query-interval

Use this command to set the *IGMP* Querier Query Interval time. It is the amount of time in seconds that the switch waits before sending another general query.

Default	Disabled
Format	`set igmp querier query-interval 1-1800`
Mode	Global Config

no set igmp querier query-interval

Use this command to set the *IGMP* Querier Query Interval time to its default value.

Format	`no set igmp querier query-interval`
Mode	Global Config

set igmp querier timer expiry

Use this command to set the *IGMP* Querier timer expiration period. It is the time period that the switch remains in Non-Querier mode once it has discovered that there is a Multicast Querier in the network.

Default	60 seconds
Format	`set igmp querier timer expiry 60-300`
Mode	Global Config

no set igmp querier timer expiry

Use this command to set the *IGMP* Querier timer expiration period to its default value.

Format	`no set igmp querier timer expiry`
Mode	Global Config

set igmp querier version

Use this command to set the *IGMP* version of the query that the snooping switch is going to send periodically.

Default	1
Format	`set igmp querier version 1-2`
Mode	Global Config

no set igmp querier version

Use this command to set the *IGMP* Querier version to its default value.

Format	`no set igmp querier version`
Mode	Global Config

set igmp querier election participate

Use this command to enable the Snooping Querier to participate in the Querier Election process when it discovers the presence of another Querier in the VLAN. When this mode is enabled, if the Snooping Querier finds that the other Querier's source address is better (less) than the Snooping Querier's address, it stops sending periodic queries. If the Snooping Querier wins the election, then it will continue sending periodic queries.

Default	Disabled
Format	`set igmp querier election participate`
Mode	VLAN Config

no set igmp querier election participate

Use this command to set the Snooping Querier not to participate in querier election but go into non-querier mode as soon as it discovers the presence of another querier in the same VLAN.

Format	`no set igmp querier election participate`
Mode	VLAN Config

show igmpsnooping querier

Use this command to display *IGMP* Snooping Querier information. Configured information is displayed whether IGMP Snooping Querier is enabled.

Format	`show igmpsnooping querier [{detail | vlan` *`vlanid`*`}]`
Mode	Privileged EXEC

When the optional argument vlanid is not used, the command displays the following information.

Column	Meaning
Admin Mode	Whether IGMP Snooping Querier is active on the switch.
Admin Version	The version of IGMP that will be used while sending out the queries.
Querier Address	The IP Address which will be used in the IPv4 header while sending out IGMP queries. It can be configured using the appropriate command.
Query Interval	The amount of time in seconds that a Snooping Querier waits before sending out the periodic general query.
Querier Timeout	The amount of time to wait in the Non-Querier operational state before moving to a Querier state.

When you specify a value for vlanid, the following additional information appears.

Column	Meaning
VLAN Admin Mode	Whether iGMP Snooping Querier is active on the VLAN.
VLAN Operational State	Whether IGMP Snooping Querier is in "Querier" or "Non-Querier" state. When the switch is in *`Querier`* state, it will send out periodic general queries. When in *`Non-Querier`* state, it will wait for moving to Querier state and does not send out any queries.

Column	Meaning
VLAN Operational Max Response Time	The time to wait before removing a Leave from a host upon receiving a Leave request. This value is calculated dynamically from the Queries received from the network. If the Snooping Switch is in Querier state, then it is equal to the configured value.
Querier Election Participation	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	The IP address of the most recent Querier from which a Query was received.
Last Querier Version	The IGMP version of the most recent Querier from which a Query was received on this VLAN.

When the optional argument detail is used, the command shows the global information and the information for all Querier-enabled VLANs.

MLD Snooping Commands

This section describes commands used for MLD Snooping. In IPv4, Layer 2 switches can use *IGMP* Snooping to limit the flooding of multicast traffic by dynamically configuring Layer 2 interfaces so that multicast traffic is forwarded only to those interfaces associated with IP multicast addresses.

In IPv6, MLD Snooping performs a similar function. With MLD Snooping, IPv6 multicast data is selectively forwarded to a list of ports that want to receive the data, instead of being flooded to all ports in a VLAN. This list is constructed by snooping IPv6 multicast control packets.

Note
This feature is available for 220 switches only.

Note
This note clarifies the prioritization of MGMD Snooping Configurations. Many of the IGMP/MLD Snooping commands are available both in the Interface and VLAN modes. Operationally the system chooses or prefers the VLAN configured values over the Interface configured values for most configurations when the interface participates in the VLAN.

set mld

This command enables MLD Snooping on the system (Global Config Mode) or an Interface (Interface Config Mode). This command also enables MLD Snooping on a particular VLAN and enables MLD Snooping on all interfaces participating in a VLAN.

If an interface has MLD Snooping enabled and you enable this interface for routing or enlist it as a member of a port-channel (*LAG*), MLD Snooping functionality is disabled on that interface. MLD Snooping functionality is re-enabled if you disable routing or remove port channel (LAG) membership from an interface that has MLD Snooping enabled.

MLD Snooping supports the following activities:

- Validation of address version, payload length consistencies and discarding of the frame upon error.
- Maintenance of the forwarding table entries based on the MAC address versus the IPv6 address.
- Flooding of unregistered multicast data packets to all ports in the VLAN.

Default	disabled
Format	`set mld vlanid`
Mode	• Global Config • Interface Config • VLAN Mode

no set mld

Use this command to disable MLD Snooping on the system.

Format	`set mld vlanid`
Mode	• Global Config • Interface Config • VLAN Mode

set mld interfacemode

Use this command to enable MLD Snooping on all interfaces. If an interface has MLD Snooping enabled and you enable this interface for routing or enlist it as a member of a port-channel (*LAG*), MLD Snooping functionality is disabled on that interface. MLD Snooping functionality is re-enabled if you disable routing or remove port-channel (LAG) membership from an interface that has MLD Snooping enabled.

Default	disabled
Format	`set mld interfacemode`
Mode	Global Config

no set mld interfacemode

Use this command to disable MLD Snooping on all interfaces.

Format	`no set mld interfacemode`
Mode	Global Config

set mld fast-leave

Use this command to enable MLD Snooping fast-leave admin mode on a selected interface or VLAN. Enabling fast-leave allows the switch to immediately remove the Layer 2 LAN interface from its

forwarding table entry upon receiving and MLD done message for that multicast group without first sending out MAC-based general queries to the interface.

Note
You should enable fast-leave admin mode only on VLANs where only one host is connected to each Layer 2 LAN port. This prevents the inadvertent dropping of the other hosts that were connected to the same layer 2 LAN port but were still interested in receiving multicast traffic directed to that group.

Note
Fast-leave processing is supported only with MLD version 1 hosts.

Default	disabled
Format	`set mld fast-leave` *`vlanid`*
Mode	• Interface Config • VLAN Mode

no set mld fast-leave

Use this command to disable MLD Snooping fast-leave admin mode on a selected interface.

Format	`no set mld fast-leave` *`vlanid`*
Mode	• Interface Config • VLAN Mode

set mld groupmembership-interval

Use this command to set the MLD Group Membership Interval time on a VLAN, one interface or all interfaces. The Group Membership Interval time is the amount of time in seconds that a switch waits for a report from a particular group on a particular interface before deleting the interface from the entry. This value must be greater than the MLDv2 Maximum Response time value. The range is 2 to 3600 seconds.

Default	260 seconds
Format	`set mld groupmembership-interval` *`vlanid 2-3600`*
Mode	• Interface Config • Global Config • VLAN Mode

no set groupmembership-interval

Use this command to set the MLDv2 Group Membership Interval time to the default value.

Format	`no set mld groupmembership-interval`
Mode	• Interface Config • Global Config • VLAN Mode

set mld maxresponse

Use this command to set the MLD Maximum Response time for the system, on a particular interface or VLAN. The Maximum Response time is the amount of time in seconds that a switch will wait after sending a query on an interface because it did not receive a report for a particular group in that interface. This value must be less than the MLD Query Interval time value. The range is 1 to 65 seconds.

Default	10 seconds
Format	`set mld maxresponse` *`1-65`*
Mode	• Global Config • Interface Config • VLAN Mode

no set mld maxresponse

Use this command to set the max response time (on the interface or VLAN) to the default value.

Format	`no set mld maxresponse`
Mode	• Global Config • Interface Config • VLAN Mode

set mld mcrtexpiretime

Use this command to set the Multicast Router Present Expiration time. The time is set for the system, on a particular interface or VLAN. This is the amount of time in seconds that a switch waits for a query to be received on an interface before the interface is removed from the list of interfaces with multicast routers attached. The range is 0 to 3600 seconds. A value of 0 indicates an infinite timeout, that is, no expiration.

Default	0
Format	`set mld mcrtexpiretime` *`vlanid 0-3600`*
Mode	• Global Config • Interface Config

no set mld mcrtexpiretime

Use this command to set the Multicast Router Present Expiration time to 0. The time is set for the system, on a particular interface or a VLAN.

Format	`no set mld mcrtexpiretime` *`vlanid`*
Mode	• Global Config • Interface Config

set mld mrouter

Use this command to configure the VLAN ID for the VLAN that has the multicast router attached mode enabled.

Format	`set mld mrouter` *`vlanid`*
Mode	Interface Config

no set mld mrouter

Use this command to disable multicast router attached mode for a VLAN with a particular VLAN ID.

Format	`no set mld mrouter` *`vlanid`*
Mode	Interface Config

set mld mrouter interface

Use this command to configure the interface as a multicast router-attached interface. When configured as a multicast router interface, the interface is treated as a multicast router-attached interface in all VLANs.

Default	disabled
Format	`set mld mrouter interface`
Mode	Interface Config

no set mld mrouter interface

Use this command to disable the status of the interface as a statically configured multicast router-attached interface.

Format	`no set mld mrouter interface`
Mode	Interface Config

show mldsnooping

Use this command to display MLD Snooping information. Configured information is displayed whether MLD Snooping is enabled.

Format	`show mldsnooping [unit/slot/port | vlanid]`
Mode	Privileged EXEC

When the optional arguments unit/slot/port or vlanid are not used, the command displays the following information.

Term	Definition
Admin Mode	Whether 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
MLD Snooping Admin Mode	Whether MLD Snooping is active on the interface.
Fast Leave Mode	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	Whether MLD Snooping is active on the VLAN.

show mldsnooping mrouter interface

Use this command to display information about statically configured multicast router attached interfaces.

Format	`show mldsnooping mrouter interface` *`unit/slot/port`*
Mode	Privileged EXEC

Term	Definition
Interface	Shows the interface on which multicast router information is being displayed.
Multicast Router Attached	Whether multicast router is statically enabled on the interface.
VLAN ID	Displays the list of VLANs of which the interface is a member.

show mldsnooping mrouter vlan

Use this command to display information about statically configured multicast router-attached interfaces.

Format	`show mldsnooping mrouter vlan` *`unit/slot/port`*
Mode	Privileged EXEC

Term	Definition
Interface	Shows the interface on which multicast router information is being displayed.
VLAN ID	Displays the list of VLANs of which the interface is a member.

show mldsnooping ssm entries

Use this command to display the source specific multicast forwarding database built by MLD snooping.

A given {Source, Group, VLAN} combination can have few interfaces in INCLUDE mode and few interfaces in EXCLUDE mode. In such instances, two rows for the same {Source, Group, VLAN} combinations are displayed.

Format	`show mldsnooping ssm entries`
Mode	Privileged EXEC

Term	Definition
VLAN	The VLAN on which the entry is learned.
Group	The IPv6 multicast group address.
Source	The IPv6 source address.

Term	Definition
Source Filter Mode	The source filter mode (Include/Exclude) for the specified group.
Interfaces	1)If Source Filter Mode is “Include,” specifies the list of interfaces on which a incoming packet is forwarded. If it’s source IP address is equal to the current entry’s Source, the destination IP address is equal to the current entry’s Group and the VLAN ID on which it arrived is current entry’s VLAN. 2) If Source Filter Mode is “Exclude,” specifies the list of interfaces on which a incoming packet is forwarded. If it’s source IP address is *not* equal to the current entry’s Source, the destination IP address is equal to current entry’s Group and VLAN ID on which it arrived is current entry’s VLAN.

show mac-address-table mldsnooping

Use this command to display the MLD Snooping entries in the Multicast Forwarding Database (MFDB) table.

Format	`show mac-address-table mldsnooping`
Mode	Privileged EXEC

Term	Definition
VLAN ID	The VLAN in which the MAC address is learned.
MAC Address	A multicast MAC address for which the switch has forwarding or filtering information. The format is 6 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB.
Type	The type of entry, which is either static (added by the user) or dynamic (added to the table as a result of a learning process or protocol.)
Description	The text description of this multicast table entry.
Interfaces	The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).

clear mldsnooping

Use this command to delete all MLD snooping entries from the MFDB table.

Format	`clear mldsnooping`
Mode	Privileged EXEC

MLD Snooping Querier Commands

In an IPv6 environment, MLD Snooping requires that one central switch or router periodically query all end-devices on the network to announce their multicast memberships. This central device is the MLD

Querier. The MLD query responses, known as MLD reports, keep the switch updated with the current multicast group membership on a port-by-port basis. If the switch does not receive updated membership information in a timely fashion, it will stop forwarding multicasts to the port where the end device is located.

This section describes the commands used to configure and display information on MLD Snooping queries on the network and, separately, on VLANs.

Note
This feature is available for 220 switches only.

Note
This note clarifies the prioritization of MGMD Snooping Configurations. Many of the *IGMP*/MLD Snooping commands are available both in the Interface and VLAN modes. Operationally the system chooses or prefers the VLAN configured values over the Interface configured values for most configurations when the interface participates in the VLAN.

set mld querier

Use this command to enable MLD Snooping Querier on the system (Global Config Mode) or on a VLAN. Using this command, you can specify the IP address that the snooping querier switch should use as a source address while generating periodic queries.

If a VLAN has MLD Snooping Querier enabled and MLD Snooping is operationally disabled on it, MLD Snooping Querier functionality is disabled on that VLAN. MLD Snooping functionality is re-enabled if MLD Snooping is operational on the VLAN.

The MLD Snooping Querier sends periodic general queries on the VLAN to solicit membership reports.

Default	disabled
Format	`set mld querier [vlan-id] [address ipv6_address]`
Mode	• Global Config • VLAN Mode

no set mld querier

Use this command to disable MLD Snooping Querier on the system. Use the optional parameter address to reset the querier address.

Format	`no set mld querier [vlan-id][address]`
Mode	• Global Config • VLAN Mode

set mld querier query_interval

Use this command to set the MLD Querier Query Interval time. It is the amount of time in seconds that the switch waits before sending another general query.

Default	60 seconds
Format	`set mld querier query_interval` *1-1800*
Mode	Global Config

no set mld querier query_interval

Use this command to set the MLD Querier Query Interval time to its default value.

Format	`no set mld querier query_interval`
Mode	Global Config

set mld querier timer expiry

Use this command to set the MLD Querier timer expiration period. It is the time period that the switch remains in Non-Querier mode once it has discovered that there is a Multicast Querier in the network.

Default	60 seconds
Format	`set mld querier timer expiry` *60-300*
Mode	Global Config

no set mld querier timer expiry

Use this command to set the MLD Querier timer expiration period to its default value.

Format	`no set mld querier timer expiry`
Mode	Global Config

set mld querier election participate

Use this command to enable the Snooping Querier to participate in the Querier Election process when it discovers the presence of another Querier in the VLAN. When this mode is enabled, if the Snooping Querier finds that the other Querier's source address is better (less) than the Snooping Querier's address, it stops sending periodic queries. If the Snooping Querier wins the election, then it will continue sending periodic queries.

Default	disabled
Format	`set mld querier election participate`
Mode	VLAN Config

no set mld querier election participate

Use this command to set the snooping querier not to participate in querier election but go into a non-querier mode as soon as it discovers the presence of another querier in the same VLAN.

Format	`no set mld querier election participate`
Mode	VLAN Config

show mldsnooping querier

Use this command to display MLD Snooping Querier information. Configured information is displayed whether MLD Snooping Querier is enabled.

Format	`show mldsnooping querier [{detail | vlan` *`vlanid`*`}]`
Mode	Privileged EXEC

When the optional arguments vlandid are not used, the command displays the following information.

Field	Description
Admin Mode	Whether MLD Snooping Querier is active on the switch.
Admin Version	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	Whether MLD Snooping Querier is active on the VLAN.
VLAN Operational State	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	The time to wait before removing a Leave from a host upon receiving a Leave request. This value is calculated dynamically from the Queries received from the network. If the Snooping Switch is in Querier state, then it is equal to the configured value.
Querier Election Participate	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	The IP address of the most recent Querier from which a Query was received.
Last Querier Version	The MLD version of the most recent Querier from which a Query was received on this VLAN.

When the optional argument detail is used, the command shows the global information and the information for all Querier-enabled VLANs.

Port Security Commands

This section describes the command used to configure Port Security on the switch. Port security, which is also known as port MAC locking, allows you to secure the network by locking allowable MAC addresses on a given port. Packets with a matching source MAC address are forwarded normally, and all other packets are discarded.

Note
To enable the *SNMP (Simple Network Management Protocol)* trap specific to port security, see snmp-server enable traps violation on page 93.

port-security

This command enables port locking on an interface, a range of interfaces, or at the system level.

Default	Disabled
Format	`port-security`
Mode	• Global Config (to enable port locking globally) • Interface Config (to enable port locking on an interface or range of interfaces)

no port-security

This command disables port locking for one (Interface Config) or all (Global Config) ports.

Format	`no port-security`
Mode	• Global Config • Interface Config

port-security max-dynamic

This command sets the maximum number of dynamically locked MAC addresses allowed on a specific port. The valid range is 0–600.

Default	600
Format	`port-security max-dynamic` *`maxvalue`*
Mode	Interface Config

no port-security max-dynamic

This command resets the maximum number of dynamically locked MAC addresses allowed on a specific port to its default value.

Format	`no port-security max-dynamic`
Mode	Interface Config

port-security max-static

This command sets the maximum number of statically locked MAC addresses allowed on a port. The valid range is 0–20.

Default	1
Format	`port-security max-static` *`maxvalue`*
Mode	Interface Config

no port-security max-static

This command sets maximum number of statically locked MAC addresses to the default value.

Format	`no port-security max-static`
Mode	Interface Config

port-security mac-address

This command adds a MAC address to the list of statically locked MAC addresses for an interface or range of interfaces. The vid is the VLAN ID.

Format	`port-security mac-address` *`mac-address vid`*
Mode	Interface Config

no port-security mac-address

This command removes a MAC address from the list of statically locked MAC addresses.

Format	`no port-security mac-address` *`mac-address vid`*
Mode	Interface Config

port-security mac-address move

This command converts dynamically locked MAC addresses to statically locked addresses for an interface or range of interfaces.

Format	`port-security mac-address move`
Mode	Interface Config

port-security mac-address sticky

This command enables sticky mode Port MAC Locking on a port. If accompanied by a MAC address and a VLAN id (for interface config mode only), it adds a sticky MAC address to the list of statically locked MAC addresses. These sticky addresses are converted back to dynamically locked addresses if sticky mode is disabled on the port. The *vid* is the VLAN ID. The Global command applies the "sticky" mode to all valid interfaces (physical and *LAG*). There is no global sticky mode as such.

Sticky addresses that are dynamically learned will appear in `show running-config` as `port-security mac-address sticky` *`mac-address vid`* entries. This distinguishes them from static entries.

Format	`port-security mac-address sticky [`*`mac-address vid`*`]`
Mode	• Global Config • Interface Config

The following shows an example of the command.

```
(Extreme 220)(Config)# port-security mac-address sticky
(Extreme 220)(Interface)# port-security mac-address sticky
(Extreme 220)(Interface)# port-security mac-address sticky
  00:00:00:00:00:01 2
```

no port-security mac-address sticky

The no form removes the sticky mode. The sticky MAC address can be deleted by using the `no port-security mac-address` command.

Format	`no port-security mac-address sticky [`*`mac-address vid`*`]`
Mode	• Global Config • Interface Config

mac-address-table limit

This command enables VLAN port security. VLAN MAC locking allows you to secure the network by locking down allowable MAC addresses on a given VLAN. Packets with a matching source MAC address can be forwarded normally. All other packets will be discarded. VLAN MAC locking will lock the dynamic MAC entries.

If VLAN and port MAC locking are enabled, VLAN MAC locking will be given precedence over port MAC locking.

Default	Disabled
Format	`mac-address-table limit [action shutdown] [notification trap ] [maximum-num] [vlan vlan-id]`
Mode	Global Config

Parameter	Description
action shutdown	After the MAC limit has been reached, the action will shut down the ports participating in the VLAN.
notification trap	Enables **snmp-server enable traps** violation on the ports participating in the VLAN. After the MAC limit has been reached, log message will be generated with the violation MAC address details.
maximum-num	MAC limit to be configured.
vlan-id	VLAN on which the MAC limit is to be applied.

The following shows an example of the command.

```
(Extreme 220) (Config) #mac-address-table limit 3 vlan 10
(Extreme 220) (Config) #mac-address-table limit action shutdown 5 vlan 20
(Extreme 220) (Config) #mac-address-table limit notification trap 4 vlan 30
(Extreme 220) (Config) #mac-address-table limit action shutdown notification trap 6 vlan
100
```

no mac-address-table limit

This command disables VLAN port security on the specified VLAN.

Default	Disabled
Format	`no mac-address-table limit [action shutdown] [notification trap ] [maximum-num] [vlan vlan-id]`
Mode	Global Config

show port-security

This command displays the port-security settings for the port(s). If you do not use a parameter, the command displays the Port Security Administrative mode. Use the optional parameters to display the settings on a specific interface or on all interfaces. Instead of 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.

Format	`show port-security [{unit/slot/port | all}]`
Mode	Privileged EXEC

Column	Meaning
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:

Column	Meaning
Admin Mode	Port Locking mode for the Interface.
Dynamic Limit	Maximum dynamically allocated MAC Addresses.
Static Limit	Maximum statically allocated MAC Addresses.
Violation Trap Mode	Whether violation traps are enabled.
Sticky Mode	The administrative mode of the port security Sticky Mode feature on the interface.

The following example shows CLI display output for the command.

```
(Extreme 220) (Routing) #show port-security 0/1
        Admin    Dynamic     Static     Violation  Sticky
Intf    Mode      Limit      Limit      Trap Mode  Mode
------  -------  ----------  ---------  ---------  --------
0/1     Disabled 1           1          Disabled   Enabled
```

show port-security dynamic

This command displays the dynamically locked MAC addresses for the port. Instead of 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.

Format	`show port-security dynamic` *`unit/slot/port`*
Mode	Privileged EXEC

Column	Meaning
MAC Address	MAC Address of dynamically locked MAC.

show port-security static

This command displays the statically locked MAC addresses for port. 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.

Format	`show port-security static {`*`unit/slot/port`* `| lag` *`lag-intf-num`*`}`
Mode	Privileged EXEC

Column	Meaning
Statically Configured MAC Address	The statically configured MAC address.
VLAN ID	The ID of the VLAN that includes the host with the specified MAC address.
Sticky	Whether the static MAC address entry is added in sticky mode.

The following example shows CLI display output for the command.

```
(Extreme 220) (Routing) #show port-security static 1/0/1
 Number of static MAC addresses configured: 2
 Statically configured MAC Address    VLAN ID    Sticky
 ---------------------------------    -------    ------
 00:00:00:00:00:01                    2            Yes
 00:00:00:00:00:02                    2            No
```

show port-security violation

This command displays the source MAC address of the last packet discarded on a locked port. Instead of 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.

Format	`show port-security violation {`*`unit/slot/port`* `| lag` *`lag-id`*`}`
Mode	Privileged EXEC

Column	Meaning
MAC Address	The source MAC address of the last frame that was discarded at a locked port.
VLAN ID	The VLAN ID, if applicable, associated with the MAC address of the last frame that was discarded at a locked port.

show mac-address-table limit

This command displays the VLAN port security configuration.

Format	`show mac-address-table limit [`*`vlan-id`*`]`
Mode	Privileged EXEC

Column	Meaning
VLAN ID	The VLAN ID on which MAC locking has been configured.

```
(Extreme 220) (Routing) #show mac-address-table limit
Vlan MAC Locking Administration Mode:  Enabled
For Vlan 10
Configured mac limit 3
Operational mac limit 3
Violation trap mode  Enabled
Violation shutdown mode  Disabled
vlan    Interface Mac-Address
------- --------- -----------------
10      0/2       00:00:00:00:44:44
10      0/2       00:00:00:00:44:45
10      0/2       00:00:00:00:44:46
For Vlan 20
Configured mac limit 3
Operational mac limit 3
Violation trap mode  Enabled
Violation shutdown mode  Disabled
vlan    Interface Mac-Address
------- --------- -----------------
```

```
20      0/28      00:00:00:00:00:11
20      0/28      00:00:00:00:00:12
20      0/28      00:00:00:00:00:13
(Extreme 220) (Routing) #show mac-address-table limit 10
Vlan MAC Locking Administration Mode:  Enabled
For Vlan 10
Configured mac limit 3
Operational mac limit 3
vlan    Interface Mac-Address
------- --------- -----------------
10      0/2       00:00:00:00:44:44
10      0/2       00:00:00:00:44:45
10      0/2       00:00:00:00:44:46
```

LLDP (802.1AB) Commands

This section describes the command used to configure *LLDP (Link Layer Discovery Protocol)*, which is defined in the IEEE 802.1AB specification. LLDP allows stations on an 802 LAN to advertise major capabilities and physical descriptions. The advertisements allow a network management system (NMS) to access and display this information.

lldp transmit

Use this command to enable the *LLDP* advertise capability on an interface or a range of interfaces.

Default	Disabled
Format	`lldp transmit`
Mode	Interface Config

no lldp transmit

Use this command to return the local data transmission capability to the default.

Format	`no lldp transmit`
Mode	Interface Config

lldp receive

Use this command to enable the *LLDP* receive capability on an interface or a range of interfaces.

Default	Disabled
Format	`lldp receive`
Mode	Interface Config

no lldp receive

Use this command to return the reception of LLDPDUs to the default value.

Format	`no lldp receive`
Mode	Interface Config

lldp timers

Use this command to set the timing parameters for local data transmission on ports enabled for *LLDP*. The interval-seconds determines the number of seconds to wait between transmitting local data LLDPDUs. The range is 1-32768 seconds. The hold-value is the multiplier on the transmit interval that sets the TTL in local data LLDPDUs. The multiplier range is 2-10. The reinit-seconds is the delay before reinitialization, and the range is 1-0 seconds.

Default	• interval—30 seconds • hold—4 • reinit—2 seconds
Format	`lldp timers [interval` *`interval-seconds`*`] [hold` *`hold-value`*`] [reinit` *`reinit-seconds`*`]`
Mode	Global Config

no lldp timers

Use this command to return any or all timing parameters for local data transmission on ports enabled for *LLDP* to the default values.

Format	`no lldp timers [interval] [hold] [reinit]`
Mode	Global Config

lldp transmit-tlv

Use this command to specify which optional type length values (TLVs) in the 802.1AB basic management set are transmitted in the LLDPDUs from an interface or range of interfaces. Use sys-name to transmit the system name TLV. To configure the system name, see snmp-server on page 92. Use sys-desc to transmit the system description TLV. Use sys-cap to transmit the system capabilities TLV. Use port-desc to transmit the port description TLV. To configure the port description, see description on page 279

Default	no optional TLVs are included
Format	`lldp transmit-tlv [sys-desc] [sys-name] [sys-cap] [port-desc]`
Mode	Interface Config

no lldp transmit-tlv

Use this command to remove an optional TLV from the LLDPDUs. Use the command without parameters to remove all optional TLVs from the LLDPDU.

Format	`no lldp transmit-tlv [sys-desc] [sys-name] [sys-cap] [port-desc]`
Mode	Interface Config

lldp transmit-mgmt

Use this command to include transmission of the local system management address information in the LLDPDUs. This command can be used to configure a single interface or a range of interfaces.

Format	`lldp transmit-mgmt`
Mode	Interface Config

no lldp transmit-mgmt

Use this command to include transmission of the local system management address information in the LLDPDUs. Use this command to cancel inclusion of the management information in LLDPDUs.

Format	`no lldp transmit-mgmt`
Mode	Interface Config

lldp notification

Use this command to enable remote data change notifications on an interface or a range of interfaces.

Default	Disabled
Format	`lldp notification`
Mode	Interface Config

no lldp notification

Use this command to disable notifications.

Default	Disabled
Format	`no lldp notification`
Mode	Interface Config

lldp notification-interval

Use this command to configure how frequently the system sends remote data change notifications. The interval parameter is the number of seconds to wait between sending notifications. The valid interval range is 5-3600 seconds.

Default	5
Format	`lldp notification-interval` *`interval`*
Mode	Global Config

no lldp notification-interval

Use this command to return the notification interval to the default value.

Format	`no lldp notification-interval`
Mode	Global Config

clear lldp statistics

Use this command to reset all *LLDP* statistics, including MED-related information.

Format	`clear lldp statistics`
Mode	Privileged EXEC

clear lldp remote-data

Use this command to delete all information from the *LLDP* remote data table, including MED-related information.

Format	`clear lldp remote-data`
Mode	Global Config

show lldp

Use this command to display a summary of the current *LLDP* configuration.

Format	`show lldp`
Mode	Privileged EXEC

Column	Meaning
Transmit Interval	How frequently the system transmits local data LLDPDUs, in seconds.
Transmit Hold Multiplier	The multiplier on the transmit interval that sets the TTL in local data LLDPDUs.
Re-initialization Delay	The delay before reinitialization, in seconds.
Notification Interval	How frequently the system sends remote data change notifications, in seconds.

show lldp interface

Use this command to display a summary of the current *LLDP* configuration for a specific interface or for all interfaces.

Format	`show lldp interface {unit/slot/port | all}`
Mode	Privileged EXEC

Column	Meaning
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.

show lldp statistics

Use this command to display the current *LLDP* traffic and remote table statistics for a specific interface or for all interfaces.

Format	`show lldp statistics {unit/slot/port | all}`
Mode	Privileged EXEC

Column	Meaning
Last Update	The amount of time since the last update to the remote table in days, hours, minutes, and seconds.
Total Inserts	Total number of inserts to the remote data table.
Total Deletes	Total number of deletes from the remote data table.
Total Drops	Total number of times the complete remote data received was not inserted due to insufficient resources.
Total Ageouts	Total number of times a complete remote data entry was deleted because the Time to Live interval expired.

The table contains the following column headings:

Column	Meaning
Interface	The interface in *unit/slot/port* format.
TX Total	Total number of LLDP packets transmitted on the port.
RX Total	Total number of LLDP packets received on the port.
Discards	Total number of LLDP frames discarded on the port for any reason.
Errors	The number of invalid LLDP frames received on the port.

Column	Meaning
Ageouts	Total number of times a complete remote data entry was deleted for the port because the Time to Live interval expired.
TVL Discards	The number of TLVs discarded.
TVL Unknowns	Total number of LLDP TLVs received on the port where the type value is in the reserved range, and not recognized.
TLV MED	The total number of LLDP-MED TLVs received on the interface.
TLV 802.1	The total number of LLDP TLVs received on the interface which are of type 802.1.
TLV 802.3	The total number of LLDP TLVs received on the interface which are of type 802.3.

show lldp remote-device

Use this command to display summary information about remote devices that transmit current *LLDP* data to the system. You can show information about LLDP remote data received on all ports or on a specific port.

Format	`show lldp remote-device {`*`unit/slot/port`* `| all}`
Mode	Privileged EXEC

Column	Meaning
Local Interface	The interface that received the LLDPDU from the remote device.
RemID	An internal identifier to the switch to mark each remote device to the system.
Chassis ID	The ID that is sent by a remote device as part of the LLDP message, it is usually a MAC address of the device.
Port ID	The port number that transmitted the LLDPDU.
System Name	The system name of the remote device.

The following example shows CLI display output for the command.

```
(Extreme 220) #show lldp remote-device all
LLDP Remote Device Summary
Local
Interface RemID    Chassis ID            Port ID             System Name
-------  -------   --------------------  ------------------  ------------------
0/1
0/2
0/3
0/4
0/5
0/6
0/7         2       00:FC:E3:90:01:0F     00:FC:E3:90:01:11
0/7         3       00:FC:E3:90:01:0F     00:FC:E3:90:01:12
0/7         4       00:FC:E3:90:01:0F     00:FC:E3:90:01:13
0/7         5       00:FC:E3:90:01:0F     00:FC:E3:90:01:14
0/7         1       00:FC:E3:90:01:0F     00:FC:E3:90:03:11
0/7         6       00:FC:E3:90:01:0F     00:FC:E3:90:04:11
0/8
0/9
0/10
0/11
```

```
0/12
--More-- or (q)uit
```

show lldp remote-device detail

Use this command to display detailed information about remote devices that transmit current *LLDP* data to an interface on the system.

Format	`show lldp remote-device detail { unit/slot/port}`
Mode	Privileged EXEC

Column	Meaning
Local Interface	The interface that received the LLDPDU from the remote device.
Remote Identifier	An internal identifier to the switch to mark each remote device to the system.
Chassis ID Subtype	The type of identification used in the Chassis ID field.
Chassis ID	The chassis of the remote device.
Port ID Subtype	The type of port on the remote device.
Port ID	The port number that transmitted the LLDPDU.
System Name	The system name of the remote device.
System Description	Describes the remote system by identifying the system name and versions of hardware, operating system, and networking software supported in the device.
Port Description	Describes the port in an alpha-numeric format. The port description is configurable.
System Capabilities Supported	The primary function(s) of the device.
System Capabilities Enabled	Shows which of the supported system capabilities are enabled.
Management Address	For each interface on the remote device with an LLDP agent, lists the type of address the remote LLDP agent uses and specifies the address used to obtain information related to the device.
Time To Live	The amount of time (in seconds) the remote device's information received in the LLDPDU should be treated as valid information.

The following example shows CLI display output for the command.

```
(Extreme 220) #show lldp remote-device detail 0/7
LLDP Remote Device Detail
Local Interface: 0/7
Remote Identifier: 2
Chassis ID Subtype: MAC Address
Chassis ID: 00:FC:E3:90:01:0F
Port ID Subtype: MAC Address
Port ID: 00:FC:E3:90:01:11
System Name:
System Description:
Port Description:
System Capabilities Supported:
System Capabilities Enabled:
Time to Live: 24 seconds
```

show lldp local-device

Use this command to display summary information about the advertised *LLDP* local data. This command can display summary information or detail for each interface.

Format	`show lldp local-device {unit/slot/port | all}`
Mode	Privileged EXEC

Column	Meaning
Interface	The interface in a *unit/slot/port* format.
Port ID	The port ID associated with this interface.
Port Description	The port description associated with the interface.

show lldp local-device detail

Use this command to display detailed information about the *LLDP* data a specific interface transmits.

Format	`show lldp local-device detail unit/slot/port`
Mode	Privileged EXEC

Column	Meaning
Interface	The interface that sends the LLDPDU.
Chassis ID Subtype	The type of identification used in the Chassis ID field.
Chassis ID	The chassis of the local device.
Port ID Subtype	The type of port on the local device.
Port ID	The port number that transmitted the LLDPDU.
System Name	The system name of the local device.
System Description	Describes the local system by identifying the system name and versions of hardware, operating system, and networking software supported in the device.
Port Description	Describes the port in an alpha-numeric format.
System Capabilities Supported	The primary function(s) of the device.
System Capabilities Enabled	Shows which of the supported system capabilities are enabled.
Management Address	The type of address and the specific address the local LLDP agent uses to send and receive information.

LLDP-MED Commands

LLDP - 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, *PoE (Power over Ethernet)* management and inventory management.

lldp med

Use this command to enable MED on an interface or a range of interfaces. By enabling MED, you will be effectively enabling the transmit and receive function of *LLDP*.

Default	Disabled
Format	`lldp med`
Mode	Interface Config

no lldp med

Use this command to disable MED.

Format	`no lldp med`
Mode	Interface Config

lldp med confignotification

Use this command to configure an interface or a range of interfaces to send the topology change notification.

Default	Disabled
Format	`lldp med confignotification`
Mode	Interface Config

no ldp med confignotification

Use this command to disable notifications.

Format	`no lldp med confignotification`
Mode	Interface Config

lldp med transmit-tlv

Use this command to specify which optional Type Length Values (TLVs) in the *LLDP* MED set will be transmitted in the Link Layer Discovery Protocol Data Units (LLDPDUs) from this interface or a range of interfaces.

Default	By default, the capabilities and network policy TLVs are included.
Format	`lldp med transmit-tlv [capabilities] [ex-pd] [ex-pse] [inventory] [location] [network-policy]`
Mode	Interface Config

Parameter	Description
capabilities	Transmit the LLDP capabilities TLV.
ex-pd	Transmit the LLDP extended PD TLV.
ex-pse	Transmit the LLDP extended PSE TLV.
inventory	Transmit the LLDP inventory TLV.
location	Transmit the LLDP location TLV.
network-policy	Transmit the LLDP network policy TLV.

no lldp med transmit-tlv

Use this command to remove a TLV.

Format	`no lldp med transmit-tlv [capabilities] [network-policy] [ex-pse] [ex-pd] [location] [inventory]`
Mode	Interface Config

lldp med all

Use this command to configure *LLDP*-MED on all the ports.

Format	`lldp med all`
Mode	Global Config

lldp med confignotification all

Use this command to configure all the ports to send the topology change notification.

Format	`lldp med confignotification all`
Mode	Global Config

lldp med faststartrepeatcount

Use this command to set the value of the fast start repeat count. [count] is the number of *LLDP* PDUs that will be transmitted when the product is enabled. The range is 1 to 10.

Default	3
Format	`lldp med faststartrepeatcount` *`[count]`*
Mode	Global Config

no lldp med faststartrepeatcount

Use this command to return to the factory default value.

Format	`no lldp med faststartrepeatcount`
Mode	Global Config

lldp med transmit-tlv all

Use this command to specify which optional Type Length Values (TLVs) in the *LLDP* MED set will be transmitted in the Link Layer Discovery Protocol Data Units (LLDPDUs).

Default	By default, the capabilities and network policy TLVs are included.
Format	`lldp med transmit-tlv all [capabilities] [ex-pd] [ex-pse] [inventory] [location] [network-policy]`
Mode	Global Config

Parameter	Description
capabilities	Transmit the LLDP capabilities TLV.
ex-pd	Transmit the LLDP extended PD TLV.
ex-pse	Transmit the LLDP extended PSE TLV.
inventory	Transmit the LLDP inventory TLV.
location	Transmit the LLDP location TLV.
network-policy	Transmit the LLDP network policy TLV.

no lldp med transmit-tlv

Use this command to remove a TLV.

Format	`no lldp med transmit-tlv [capabilities] [network-policy] [ex-pse] [ex-pd] [location] [inventory]`
Mode	Global Config

show lldp med

Use this command to display a summary of the current *LLDP* MED configuration.

Format	`show lldp med`
Mode	Privileged EXEC

The following example shows CLI display output for the command.

```
(Extreme 220) (Routing) #show lldp med
LLDP MED Global Configuration
Fast Start Repeat Count: 3
Device Class: Network Connectivity
(Extreme 220) (Routing) #
```

show lldp med interface

Use this command to display a summary of the current *LLDP* MED configuration for a specific interface. unit/slot/port indicates a specific physical interface. all indicates all valid LLDP interfaces.

Format	`show lldp med interface {`*`unit/slot/port`*` | all}`
Mode	Privileged EXEC

The following example shows CLI display output for the command.

```
(Extreme 220) (Routing) #show lldp med interface all
Interface  Link    configMED operMED   ConfigNotify TLVsTx
---------  ------  --------- --------  ------------ -----------
1/0/1      Down    Disabled  Disabled  Disabled     0,1
1/0/2      Up      Disabled  Disabled  Disabled     0,1
1/0/3      Down    Disabled  Disabled  Disabled     0,1
1/0/4      Down    Disabled  Disabled  Disabled     0,1
1/0/5      Down    Disabled  Disabled  Disabled     0,1
1/0/6      Down    Disabled  Disabled  Disabled     0,1
1/0/7      Down    Disabled  Disabled  Disabled     0,1
1/0/8      Down    Disabled  Disabled  Disabled     0,1
1/0/9      Down    Disabled  Disabled  Disabled     0,1
1/0/10     Down    Disabled  Disabled  Disabled     0,1
1/0/11     Down    Disabled  Disabled  Disabled     0,1
1/0/12     Down    Disabled  Disabled  Disabled     0,1
1/0/13     Down    Disabled  Disabled  Disabled     0,1
1/0/14     Down    Disabled  Disabled  Disabled     0,1
TLV Codes: 0- Capabilities,       1- Network Policy
           2- Location,           3- Extended PSE
           4- Extended Pd,        5- Inventory
--More-- or (q)uit
(Extreme 220) (Routing) #show lldp med interface 1/0/2
Interface  Link    configMED operMED   ConfigNotify TLVsTx
---------  ------  --------- --------  ------------ -----------
1/0/2      Up      Disabled  Disabled  Disabled     0,1
TLV Codes: 0- Capabilities,       1- Network Policy
           2- Location,           3- Extended PSE
           4- Extended Pd,        5- Inventory
(Extreme 220) (Routing) #
```

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.

Format	`show lldp med local-device detail` *`unit/slot/port`*
Mode	Privileged EXEC

The following example shows CLI display output for the command.

```
(Extreme 220) (Routing) #show lldp med local-device detail 1/0/8
LLDP MED Local Device Detail
Interface: 1/0/8
Network Policies
Media Policy Application Type : voice
Vlan ID: 10
Priority: 5
DSCP: 1
Unknown: False
Tagged: True
Media Policy Application Type : streamingvideo
Vlan ID: 20
Priority: 1
DSCP: 2
Unknown: False
Tagged: True
Inventory
Hardware Rev: xxx xxx xxx
Firmware Rev: xxx xxx xxx
Software Rev: xxx xxx xxx
Serial Num: xxx xxx xxx
Mfg Name: xxx xxx xxx
Model Name: xxx xxx xxx
Asset ID: xxx xxx xxx
Location
Subtype: elin
Info: xxx xxx xxx
Extended POE
Device Type: pseDevice
Extended POE PSE
Available: 0.3 Watts
Source: primary
Priority: critical
Extended POE PD
Required: 0.2 Watts
Source: local
Priority: low
```

show lldp med remote-device

Use this command to display the summary information about remote devices that transmit current *LLDP* MED data to the system. You can show information about LLDP MED remote data received on all valid LLDP interfaces or on a specific physical interface.

Format	`show lldp med remote-device {`*`unit/slot/port`* `| all}`
Mode	Privileged EXEC

Column	Meaning
Local Interface	The interface that received the LLDPDU from the remote device.
Remote ID	An internal identifier to the switch to mark each remote device to the system.
Device Class	Device classification of the remote device.

The following example shows CLI display output for the command.

```
(Extreme 220) (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 Con
```

show lldp med remote-device detail

Use this command to display detailed information about remote devices that transmit current *LLDP* MED data to an interface on the system.

Format	`show lldp med remote-device detail` *unit/slot/port*
Mode	Privileged EXEC

The following example shows CLI display output for the command.

```
(Extreme 220) (Routing) #show lldp med remote-device detail 1/0/8
LLDP MED Remote Device Detail
Local Interface: 1/0/8
Remote Identifier: 18
Capabilities
MED Capabilities Supported: capabilities, networkpolicy, location, extendedpse
MED Capabilities Enabled: capabilities, networkpolicy
Device Class: Endpoint Class I
Network Policies
Media Policy Application Type : voice
Vlan ID: 10
Priority: 5
DSCP: 1
Unknown: False
Tagged: True
Media Policy Application Type : streamingvideo
Vlan ID: 20
Priority: 1
DSCP: 2
Unknown: False
Tagged: True
Inventory
Hardware Rev: xxx xxx xxx
Firmware Rev: xxx xxx xxx
Software Rev: xxx xxx xxx
Serial Num: xxx xxx xxx
Mfg Name: xxx xxx xxx
Model Name: xxx xxx xxx
Asset ID: xxx xxx xxx
Location
Subtype: elin
Info: xxx xxx xxx
Extended POE
Device Type: pseDevice
Extended POE PSE
Available: 0.3 Watts
Source: primary
Priority: critical
Extended POE PD
Required: 0.2 Watts
Source: local
Priority: low
```

Denial of Service Commands

Note
Denial of Service (DataPlane) is supported on XGS-III and later platforms only.

This section describes the commands used to configure Denial of Service (DoS) Control. 200 Series software provides support for classifying and blocking specific types of Denial of Service attacks. You can configure your system to monitor and block these types of attacks:

SIP = DIP	Source IP address = Destination IP address
First Fragment	TCP Header size smaller than configured value
TCP Fragment	Allows the device to drop packets that have a TCP payload where the IP payload length minus the IP header size is less than the minimum allowed TCP header size
TCP Flag	TCP Flag SYN set and Source Port < 1024 or TCP Control Flags = 0 and TCP Sequence Number = 0 or TCP Flags FIN, URG, and PSH set and TCP Sequence Number = 0 or TCP Flags SYN and FIN set
L4 Port	Source TCP/UDP Port = Destination TCP/UDP Port
ICMP	Limiting the size of *ICMP (Internet Control Message Protocol)* Ping packets

dos-control all

This command enables Denial of Service protection checks globally.

Default	Disabled
Format	`dos-control all`
Mode	Global Config

no dos-control all

This command disables Denial of Service prevention checks globally.

Format	`no dos-control all`
Mode	Global Config

dos-control sipdip

This command enables Source IP address = Destination IP address (SIP = DIP) Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress with SIP = DIP, the packets will be dropped if the mode is enabled.

Default	Disabled
Format	`dos-control sipdip`
Mode	Global Config

no dos-control sipdip

This command disables Source IP address = Destination IP address (SIP = DIP) Denial of Service prevention.

Format	`no dos-control sipdip`
Mode	Global Config

dos-control firstfrag

This command enables Minimum TCP Header Size Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having a TCP Header Size smaller then the configured value, the packets will be dropped if the mode is enabled. The default is disabled. If you enable dos-control firstfrag, but do not provide a Minimum TCP Header Size, the system sets that value to 20.

Default	Disabled (20)
Format	`dos-control firstfrag [0-255]`
Mode	Global Config

no dos-control firstfrag

This command sets Minimum TCP Header Size Denial of Service protection to the default value of disabled.

Format	`no dos-control firstfrag`
Mode	Global Config

dos-control tcpfrag

This command enables TCP Fragment Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack and packets that have a TCP payload in which the IP payload length minus the IP header size is less than the minimum allowed TCP header size are dropped.

Default	Disabled
Format	`dos-control tcpfrag`
Mode	Global Config

no dos-control tcpfrag

This command disables TCP Fragment Denial of Service protection.

Format	`no dos-control tcpfrag`
Mode	Global Config

dos-control tcpflag

This command enables TCP Flag Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attacks. If packets ingress having TCP Flag SYN set and a source port less than 1024 or having TCP Control Flags set to 0 and TCP Sequence Number set to 0 or having TCP Flags FIN, URG, and PSH set and TCP Sequence Number set to 0 or having TCP Flags SYN and FIN both set, the packets will be dropped if the mode is enabled.

Default	Disabled
Format	`dos-control tcpflag`
Mode	Global Config

no dos-control tcpflag

This command sets disables TCP Flag Denial of Service protections.

Format	`no dos-control tcpflag`
Mode	Global Config

dos-control l4port

This command enables L4 Port Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having Source TCP/UDP Port Number equal to Destination TCP/UDP Port Number, the packets will be dropped if the mode is enabled.

Note

Some applications mirror source and destination L4 ports - *RIP (Routing Information Protocol)* for example uses 520 for both. If you enable dos-control l4port, applications such as RIP may experience packet loss which would render the application inoperable.

Default	Disabled
Format	`dos-control l4port`
Mode	Global Config

no dos-control l4port

This command disables L4 Port Denial of Service protections.

Format	`no dos-control l4port`
Mode	Global Config

dos-control smacdmac

This command enables Source MAC address = Destination MAC address (SMAC = DMAC) Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress with SMAC = DMAC, the packets will be dropped if the mode is enabled.

Default	Disabled
Format	`dos-control smacdmac`
Mode	Global Config

no dos-control smacdmac

This command disables Source MAC address = Destination MAC address (SMAC = DMAC) DoS protection.

Format	`no dos-control smacdmac`
Mode	Global Config

dos-control tcpport

Note
This command is only supported on the BCM56224, BCM56514, BCM56624, BCM56634, BCM56636 and BCM56820 and BCM5621x 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
Format	`dos-control tcpport`
Mode	Global Config

no dos-control tcpport

This command disables TCP L4 source = destination port number (Source TCP Port = Destination TCP Port) Denial of Service protection.

Format	`no dos-control tcpport`
Mode	Global Config

dos-control udpport

Note
This command is only supported on the BCM56224, BCM56514, BCM56624, BCM56634, BCM56636 and BCM56820 and BCM5621x 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
Format	`dos-control udpport`
Mode	Global Config

no dos-control udpport

This command disables UDP L4 source = destination port number (Source UDP Port = Destination UDP Port) Denial of Service protection.

Format	`no dos-control udpport`
Mode	Global Config

dos-control tcpflagseq

Note
This command is only supported on the BCM56224, BCM56514, BCM56624, BCM56634, BCM56636 and BCM56820 and BCM5621x 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
Format	`dos-control tcpflagseq`
Mode	Global Config

no dos-control tcpflagseq

This command sets disables TCP Flag and Sequence Denial of Service protection.

Format	`no dos-control tcpflagseq`
Mode	Global Config

dos-control tcpoffset

Note
This command is only supported on the BCM56224, BCM56514, BCM56624, BCM56634, BCM56636 and BCM56820 and BCM5621x 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
Format	`dos-control tcpoffset`
Mode	Global Config

no dos-control tcpoffset

This command disabled TCP Offset Denial of Service protection.

Format	`no dos-control tcpoffset`
Mode	Global Config

dos-control tcpsyn

Note
This command is only supported on the BCM56224, BCM56514, BCM56624, BCM56634, BCM56636 and BCM56820 and BCM5621x 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
Format	`dos-control tcpsyn`
Mode	Global Config

no dos-control tcpsyn

This command sets disables TCP SYN and L4 source = 0-1023 Denial of Service protection.

Format	`no dos-control tcpsyn`
Mode	Global Config

dos-control tcpsynfin

Note
This command is only supported on the BCM56224, BCM56514, BCM56624, BCM56634, BCM56636 and BCM56820 and BCM5621x 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
Format	`dos-control tcpsynfin`
Mode	Global Config

no dos-control tcpsynfin

This command sets disables TCP SYN & FIN Denial of Service protection.

Format	`no dos-control tcpsynfin`
Mode	Global Config

dos-control tcpfinurgpsh

Note
This command is only supported on the BCM56224, BCM56514, BCM56624, BCM56634, BCM56636 and BCM56820 and BCM5621x 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
Format	`dos-control tcpfinurgpsh`
Mode	Global Config

no dos-control tcpfinurgpsh

This command sets disables TCP FIN and URG and PSH and SEQ = 0 checking Denial of Service protections.

Format	`no dos-control tcpfinurgpsh`
Mode	Global Config

dos-control icmpv4

Note
This command is only supported on the BCM56224, BCM56514, BCM56624, BCM56634, BCM56636 and BCM56820 and BCM5621x 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)
Format	`dos-control icmpv4 [0-16376]`
Mode	Global Config

no dos-control icmpv4

This command disables Maximum *ICMP* Packet Size Denial of Service protections.

Format	`no dos-control icmpv4`
Mode	Global Config

dos-control icmpv6

Note
This command is only supported on the BCM56224, BCM56514, BCM56624, BCM56634, BCM56636 and BCM56820 and BCM5621x 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)
Format	`dos-control icmpv6 0-16376`
Mode	Global Config

no dos-control icmpv6

This command disables Maximum *ICMP* Packet Size Denial of Service protections.

Format	`no dos-control icmpv6`
Mode	Global Config

dos-control icmpfrag

Note
This command is only supported on the BCM56224, BCM56514, BCM56624, BCM56634, BCM56636 and BCM56820 and BCM5621x 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
Format	`dos-control icmpfrag`
Mode	Global Config

no dos-control icmpfrag

This command disabled *ICMP* Fragment Denial of Service protection.

Format	`no dos-control icmpfrag`
Mode	Global Config

show dos-control

This command displays Denial of Service configuration information.

Format	`show dos-control`
Mode	Privileged EXEC

Note
Some of the following information displays only if you are using the BCM56224, BCM56514, BCM56624, BCM56634, BCM56636 and BCM56820 and BCM5621x platforms.

Column	Meaning
First Fragment Mode	The administrative mode of First Fragment DoS prevention. When enabled, this causes the switch to drop packets that have a TCP header smaller then the configured Min TCP Hdr Size.
Min TCP Hdr Size	The minimum TCP header size the switch will accept if First Fragment DoS prevention is enabled.
ICMPv4 Mode	The administrative mode of ICMPv4 DoS prevention. When enabled, this causes the switch to drop *ICMP* packets that have a type set to ECHO_REQ (ping) and a size greater than the configured ICMPv4 Payload Size.
Max ICMPv4 Payload Size	The maximum ICMPv4 payload size to accept when ICMPv4 DoS protection is enabled.
ICMPv6 Mode	The administrative mode of ICMPv6 DoS prevention. When enabled, this causes the switch to drop ICMP packets that have a type set to ECHO_REQ (ping) and a size greater than the configured ICMPv6 Payload Size.

Column	Meaning
Max ICMPv6 Payload Size	The maximum ICMPv6 payload size to accept when ICMPv6 DoS protection is enabled.
ICMPv4 Fragment Mode	The administrative mode of ICMPv4 Fragment DoS prevention. When enabled, this causes the switch to drop fragmented ICMPv4 packets.
TCP Port Mode	The administrative mode of TCP Port DoS prevention. When enabled, this causes the switch to drop packets that have the TCP source port equal to the TCP destination port.
UDP Port Mode	The administrative mode of UDP Port DoS prevention. When enabled, this causes the switch to drop packets that have the UDP source port equal to the UDP destination port.
SIPDIP Mode	The administrative mode of SIP=DIP DoS prevention. Enabling this causes the switch to drop packets that have a source IP address equal to the destination IP address. The factory default is disabled.
SMACDMAC Mode	The administrative mode of SMAC=DMAC DoS prevention. Enabling this causes the switch to drop packets that have a source MAC address equal to the destination MAC address.
TCP FIN&URG& PSH Mode	The administrative mode of TCP FIN & URG & PSH DoS prevention. Enabling this causes the switch to drop packets that have TCP flags FIN, URG, and PSH set and TCP Sequence Number = 0.
TCP Flag & Sequence Mode	The administrative mode of TCP Flag DoS prevention. Enabling this causes the switch to drop packets that have TCP control flags set to 0 and TCP sequence number set to 0.
TCP SYN Mode	The administrative mode of TCP SYN DoS prevention. Enabling this causes the switch to drop packets that have TCP Flags SYN set.
TCP SYN & FIN Mode	The administrative mode of TCP SYN & FIN DoS prevention. Enabling this causes the switch to drop packets that have TCP Flags SYN and FIN set.
TCP Fragment Mode	The administrative mode of TCP Fragment DoS prevention. Enabling this causes the switch to drop packets that have a TCP payload in which the IP payload length minus the IP header size is less than the minimum allowed TCP header size.
TCP Offset Mode	The administrative mode of TCP Offset DoS prevention. Enabling this causes the switch to drop packets that have a TCP header Offset equal to 1.

MAC Database Commands

This section describes the commands used to configure and view information about the MAC databases.

bridge aging-time

This command configures the forwarding database address aging timeout in seconds. The seconds parameter must be within the range of 10 to 1,000,000 seconds. In an SVL system, the [fdbid/all] parameter is not used and will be ignored if entered. In an SVL system, the [fdbid/all] parameter is not used and will be ignored if entered.

Default	300
Format	`bridge aging-time` *`10-1,000,000`*
Mode	Global Config

no bridge aging-time

This command sets the forwarding database address aging timeout to the default value. In an SVL system, the [fdbid/all] parameter is not used and will be ignored if entered.

Format	`no bridge aging-time`
Mode	Global Config

show forwardingdb agetime

This command displays the timeout for address aging.

Default	all
Format	`show forwardingdb agetime`
Mode	Privileged EXEC

Column	Meaning
Address Aging Timeout	Displays the system's address aging timeout value in seconds.

show mac-address-table multicast

This command displays the Multicast Forwarding Database (MFDB) information. If you enter the command with no parameter, the entire table is displayed. You can display the table entry for one MAC Address by specifying the MAC address as an optional parameter.

Format	`show mac-address-table multicast` *`macaddr`*
Mode	Privileged EXEC

Column	Meaning
VLAN ID	The VLAN in which the MAC address is learned.
MAC Address	A multicast MAC address for which the switch has forwarding or filtering information. The format is 6 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB.
Source	The component that is responsible for this entry in the Multicast Forwarding Database. The source can be *IGMP* Snooping, GMRP, and Static Filtering.
Type	The type of the entry. Static entries are those that are configured by the end user. Dynamic entries are added to the table as a result of a learning process or protocol.
Description	The text description of this multicast table entry.
Interfaces	The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).
Fwd Interface	The resultant forwarding list is derived from combining all the component's forwarding interfaces and removing the interfaces that are listed as the static filtering interfaces.

If one or more entries exist in the multicast forwarding table, the command output looks similar to the following:

```
(Extreme 220) (Routing) #show mac-address-table multicast
                                                                    Fwd
VLAN ID MAC Address       Source  Type    Description     Interface Interface
------- ----------------- ------- ------- --------------- --------- ---------
1       01:00:5E:01:02:03 Filter  Static  Mgmt Config     Fwd:      Fwd:
                                                          1/0/1,    1/0/1,
                                                          1/0/2,    1/0/2,
                                                          1/0/3,    1/0/3,
                                                          1/0/4,    1/0/4,
                                                          1/0/5,    1/0/5,
                                                          1/0/6,    1/0/6,
                                                          1/0/7,    1/0/7,
                                                          1/0/8,    1/0/8,
                                                          1/0/9,    1/0/9,
                                                          1/0/10,   1/0/10,
--More-- or (q)uit
```

show mac-address-table stats

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

Format	`show mac-address-table stats`
Mode	Privileged EXEC

Column	Meaning
Total Entries	The total number of entries that can possibly be in the Multicast Forwarding Database table.
Most MFDB Entries Ever Used	The largest number of entries that have been present in the Multicast Forwarding Database table. This value is also known as the MFDB high-water mark.
Current Entries	The current number of entries in the MFDB.

ISDP Commands

This section describes the commands used to configure the industry standard Discovery Protocol (ISDP).

isdp run

This command enables ISDP on the switch.

Default	Enabled
Format	`isdp run`
Mode	Global Config

no isdp run

This command disables ISDP on the switch.

Format	`no isdp run`
Mode	Global Config

isdp holdtime

This command configures the hold time for ISDP packets that the switch transmits. The hold time specifies how long a receiving device should store information sent in the ISDP packet before discarding it. The range is given in seconds.

Default	180 seconds
Format	`isdp holdtime` *`10-255`*
Mode	Global Config

isdp timer

This command sets the period of time between sending new ISDP packets. The range is given in seconds.

Default	60 seconds
Format	`isdp timer` *`5-254`*
Mode	Global Config

isdp advertise-v2

This command enables the sending of ISDP version 2 packets from the device.

Default	Enabled
Format	`isdp advertise-v2`
Mode	Global Config

no isdp advertise-v2

This command disables the sending of ISDP version 2 packets from the device.

Format	`no isdp advertise-v2`
Mode	Global Config

isdp enable

This command enables ISDP on an interface or range of interfaces.

Note

ISDP must be enabled both globally and on the interface in order for the interface to transmit ISDP packets. If ISDP is globally disabled on the switch, the interface will not transmit ISDP packets, regardless of the ISDP status on the interface. To enable ISDP globally, use the command isdp run on page 485.

Default	Enabled
Format	`isdp enable`
Mode	Interface Config

no isdp enable

This command disables ISDP on the interface.

Format	`no isdp enable`
Mode	Interface Config

clear isdp counters

This command clears ISDP counters.

Format	`clear isdp counters`
Mode	Privileged EXEC

clear isdp table

This command clears entries in the ISDP table.

Format	`clear isdp table`
Mode	Privileged EXEC

show isdp

This command displays global ISDP settings.

Format	`show isdp`
Mode	Privileged EXEC

Term	Definition
Timer	The frequency with which this device sends ISDP packets. This value is given in seconds.
Hold Time	The length of time the receiving device should save information sent by this device. This value is given in seconds.
Version 2 Advertisements	The setting for sending ISDPv2 packets. If disabled, version 1 packets are transmitted.
Neighbors table time since last change	The amount of time that has passed since the ISPD neighbor table changed.
Device ID	The Device ID advertised by this device. The format of this Device ID is characterized by the value of the Device ID Format object.
Device ID Format Capability	The Device ID format capability of the device. • serialNumber indicates that the device uses a serial number as the format for its Device ID. • macAddress indicates that the device uses a Layer 2 MAC address as the format for its Device ID. • other indicates that the device uses its platform-specific format as the format for its Device ID.
Device ID Format	The Device ID format of the device. • serialNumber indicates that the value is in the form of an ASCII string containing the device serial number. • macAddress indicates that the value is in the form of a Layer 2 MAC address. • other indicates that the value is in the form of a platform specific ASCII string containing info that identifies the device. For example, ASCII string contains serialNumber appended/prepended with system name.

The following example shows CLI display output for the command.

```
(Extreme 220) (Routing) #show isdp
Timer..................................... 30
Hold Time................................. 180
Version 2 Advertisements.................. Enabled
Neighbors table time since last change..... 0 days 00:00:00
Device ID................................. 1114728
Device ID format capability............... Serial Number, Host Name
Device ID format.......................... Serial Number
```

show isdp interface

This command displays ISDP settings for the specified interface.

Format	`show isdp interface {all | unit/slot/port}`
Mode	Privileged EXEC

Term	Definition
Interface	The unit/slot/port of the specified interface.
Mode	ISDP mode enabled/disabled status for the interface(s).

The following example shows CLI display output for the command.

```
(Extreme 220) (Routing) #show isdp interface 0/1
Interface        Mode
---------------  ----------
0/1              Enabled
```

The following example shows CLI display output for the command.

```
(Extreme 220) (Routing) #show isdp interface all
Interface        Mode
---------------  ----------
0/1                 Enabled
0/2                 Enabled
0/3                 Enabled
0/4                 Enabled
0/5                 Enabled
0/6                 Enabled
0/7                 Enabled
0/8                 Enabled
```

show isdp entry

This command displays ISDP entries. If the device id is specified, then only entries for that device are shown.

Format	`show isdp entry {all | deviceid}`
Mode	Privileged EXEC

Term	Definition
Device ID	The device ID associated with the neighbor which advertised the information.
IP Addresses	The IP address(es) associated with the neighbor.
Capability	ISDP Functional Capabilities advertised by the neighbor.
Platform	The hardware platform advertised by the neighbor.
Interface	The interface (unit/slot/port) on which the neighbor's advertisement was received.
Port ID	The port ID of the interface from which the neighbor sent the advertisement.
Hold Time	The hold time advertised by the neighbor.
Version	The software version that the neighbor is running.

Term	Definition
Advertisement Version	The version of the advertisement packet received from the neighbor.
Entry Last Changed Time	The time when the entry was last changed.

The following example shows CLI display output for the command.

```
(Extreme 220) #show isdp entry Switch
Device ID                                    Switch
Address(es):
    IP Address:                               172.20.1.18
    IP Address:                               172.20.1.18
Capability                                   Router IGMP
Platform                                    cisco WS-C4948
Interface                                    0/1
Port ID                                     GigabitEthernet1/1
Holdtime                                     64
Advertisement Version                                   2
Entry last changed time                                   0 days 00:13:50
```

show isdp neighbors

This command displays the list of neighboring devices.

Format	`show isdp neighbors [{`*`unit/slot/port`*` | detail}]`
Mode	Privileged EXEC

Term	Definition
Device ID	The device ID associated with the neighbor which advertised the information.
IP Addresses	The IP addresses associated with the neighbor.
Capability	ISDP functional capabilities advertised by the neighbor.
Platform	The hardware platform advertised by the neighbor.
Interface	The interface (*`unit/slot/port`*) on which the neighbor's advertisement was received.
Port ID	The port ID of the interface from which the neighbor sent the advertisement.
Hold Time	The hold time advertised by the neighbor.
Advertisement Version	The version of the advertisement packet received from the neighbor.
Entry Last Changed Time	Time when the entry was last modified.
Version	The software version that the neighbor is running.

The following example shows CLI display output for the command.

```
(Extreme 220) #show isdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge,
                  S - Switch, H - Host, I - IGMP, r - Repeater
 Device ID           Intf Holdtime  Capability   Platform       Port ID
-------------------- ----- --------- ------------ -------------------- --------------------
Switch               0/1   165       RI               cisco WS-C4948    GigabitEthernet1/1
```

The following example shows CLI display output for the command.

```
(Extreme 220) #show isdp neighbors detail
Device ID                                              0001f45f1bc0
Address(es):
    IP Address:                                        10.27.7.57
Capability                                             Router Trans Bridge Switch IGMP
Platform                                               SecureStack C2
Interface                                              0/48
Port ID                                                ge.3.14
Holdtime                                               131
Advertisement Version                                  2
Entry last changed time                                0 days 00:01:59
Version:                                               05.00.56
```

show isdp traffic

This command displays ISDP statistics.

Format	show isdp traffic
Mode	Privileged EXEC

Term	Definition
ISDP Packets Received	Total number of ISDP packets received
ISDP Packets Transmitted	Total number of ISDP packets transmitted
ISDPv1 Packets Received	Total number of ISDPv1 packets received
ISDPv1 Packets Transmitted	Total number of ISDPv1 packets transmitted
ISDPv2 Packets Received	Total number of ISDPv2 packets received
ISDPv2 Packets Transmitted	Total number of ISDPv2 packets transmitted
ISDP Bad Header	Number of packets received with a bad header
ISDP Checksum Error	Number of packets received with a checksum error
ISDP Transmission Failure	Number of packets which failed to transmit
ISDP Invalid Format	Number of invalid packets received
ISDP Table Full	Number of times a neighbor entry was not added to the table due to a full database

Term	Definition
ISDP IP Address Table Full	Displays the number of times a neighbor entry was added to the table without an IP address.

The following example shows CLI display output for the command.

```
(Extreme 220) (Routing) #show isdp traffic
ISDP Packets Received..........................4253
ISDP Packets Transmitted.......................127
ISDPv1 Packets Received........................0
ISDPv1 Packets Transmitted.....................0
ISDPv2 Packets Received........................4253
ISDPv2 Packets Transmitted.....................4351
ISDP Bad Header................................0
ISDP Checksum Error............................0
ISDP Transmission Failure......................0
ISDP Invalid Format............................0
ISDP Table Full................................392
ISDP IP Address Table Full.....................737
```

debug isdp packet

This command enables tracing of ISDP packets processed by the switch. ISDP must be enabled on both the device and the interface in order to monitor packets for a particular interface.

Format	`debug isdp packet [{receive | transmit}]`
Mode	Privileged EXEC

no debug isdp packet

This command disables tracing of ISDP packets on the receive or the transmit sides or on both sides.

Format	`no debug isdp packet [{receive | transmit}]`
Mode	Privileged EXEC

Interface Error Disable and Auto Recovery

Interface error disable automatically disables an interface when an error is detected; no traffic is allowed until the interface is either manually re-enabled or, if auto recovery is configured, the configured auto recovery time interval has passed.

For interface error disable and auto recovery, an error condition is detected for an interface, the interface is placed in a diagnostic disabled state by shutting down the interface. The error disabled interface does not allow any traffic until the interface is re-enabled. The error disabled interface can be manually enabled. Alternatively administrator can enable auto recovery feature. 200 Series Auto Recovery re-enables the interface after the expiry of configured time interval.

errdisable recovery cause

Use this command to enable auto recovery for a specified cause or all causes. When auto recovery is enabled, ports in the diag-disable state are recovered (link up) when the recovery interval expires. If the interface continues to experience errors, the interface may be placed back in the diag-disable state and disabled (link down). Interfaces in the diag-disable state can be manually recovered by entering the `no shutdown` command for the interface.

Default	None
Format	`errdisable recovery cause {all | arp-inspection | bpduguard | dhcp-rate-limit | sfp-mismatch | udld | ucast-storm | bcast-storm | mcast-storm | bpdustorm | keep-alive | mac-locking | denial-of-service}`
Mode	Global Config

no errdisable recovery cause

Use this command to disable auto recovery for a specific cause. When disabled, auto recovery will not occur for interfaces in a diag-disable state due to that cause.

Format	`no errdisable recovery cause {all | arp-inspection | bpduguard | dhcp-rate-limit | sfp-mismatch | udld | ucast-storm | bcast-storm | mcast-storm | bpdustorm | keep-alive | mac-locking | denial-of-service}`
Mode	Global Config

errdisable recovery interval

Use this command to configure the auto recovery time interval. The auto recovery time interval is common for all causes. The time can be any value from 30 to 86400 seconds.When the recovery interval expires, the system attempts to bring interfaces in the diag-disable state back into service (link up).

Default	300
Format	`errdisable recovery interval` *`30-86400`*
Mode	Global Config

no errdisable recovery interval

Use this command to reset the auto recovery interval to the factory default value of 300.

Format	`no errdisable recovery interval`
Mode	Global Config

show errdisable recovery

Use this command to display the errdisable configuration status of all configurable causes.

Format	`show errdisable recovery`
Mode	Privileged EXEC

The following information is displayed.

Column	Meaning
arp-inspection	Enable/Disable status of arp-inspection auto recovery.
bpdguard	Enable/Disable status of bpduguard auto recovery.
dhcp-rate-limit	Enable/Disable status of dhcp-rate-limit auto recovery.
sfp-mismatch	Enable/Disable status of sfp-mismatch auto recovery.
udld	Enable/Disable status of UDLD auto recovery.
bpdustorm	Enable/Disable status of bpdustorm auto recovery.
keepalive	Enable/Disable status of keepalive auto recovery.
mac-locking	Enable/Disable status of MAC locking auto recovery.
denial-of-service	Enable/Disable status of DoS auto recovery.
time interval	Time interval for auto recovery in seconds.

```
(Extreme 220) (Routing) #show errdisable recovery
Errdisable Reason      Auto-recovery Status
------------------     --------------------
dhcp-rate-limit           Disabled
arp-inspection            Disabled
udld                      Disabled
bpduguard                 Disabled
bpdustorm                 Disabled
sfp-mismatch              Disabled
keepalive                 Disabled
mac-locking               Disabled
denial-of-service         Disabled
Timeout for Auto-recovery from D-Disable state  300
```

show interfaces status err-disabled

Use this command to display the interfaces that are error disabled and the amount of time remaining for auto recovery.

Format	`show interfaces status err-disabled`
Mode	Privileged EXEC

The following information is displayed.

Column	Meaning
interface	An interface that is error disabled.
Errdisable Reason	The cause of the interface being error disabled.

Column	Meaning
Auto-Recovery Time Left	The amount of time left before auto recovery begins.

```
(Extreme 220) (Routing) #show interfaces status err-disabled
Interface      Errdisable Reason      Auto-Recovery Time Left(sec)
----------       -----------------   ------------------
0/1             udld                 279
0/2             bpduguard            285
0/3             bpdustorm            291
0/4             keepalive            11
```

UniDirectional Link Detection Commands

The purpose of the UniDirectional Link Detection (UDLD) feature is to detect and avoid unidirectional links. A unidirectional link is a forwarding anomaly in a Layer 2 communication channel in which a bi-directional link stops passing traffic in one direction. Use the UDLD commands to detect unidirectional links' physical ports. UDLD must be enabled on both sides of the link in order to detect a unidirectional link. The UDLD protocol operates by exchanging packets containing information about neighboring devices.

udld enable (Global Config)

This command enables UDLD globally on the switch.

Default	Disabled
Format	`udld enable`
Mode	Global Config

no udld enable (Global Config)

This command disables udld globally on the switch.

Format	`no udld enable`
Mode	Global Config

udld message time

This command configures the interval between UDLD probe messages on ports that are in the advertisement phase. The range is from 7 to 90 seconds.

Default	15 seconds
Format	`udld message time interval`
Mode	Global Config

udld timeout interval

This command configures the time interval after which UDLD link is considered to be unidirectional. The range is from 5 to 60 seconds.

Default	5 seconds
Format	`udld timeout interval interval`
Mode	Global Config

udld reset

This command resets all interfaces that have been shutdown by UDLD.

Default	None
Format	`udld reset`
Mode	Privileged EXEC

udld enable (Interface Config)

This command enables UDLD on the specified interface.

Default	Disabled
Format	`udld enable`
Mode	Interface Config

no udld enable (Interface Config)

This command disables UDLD on the specified interface.

Format	`no udld enable`
Mode	Interface Config

udld port

This command selects the UDLD mode operating on this interface. If the keyword **`aggressive`** is not entered, the port operates in normal mode.

Default	normal
Format	`udld port [aggressive]`
Mode	Interface Config

show udld

This command displays the global settings of UDLD.

Format	`show udld`
Mode	• User EXEC • Privileged EXEC

Column	Meaning
Admin Mode	The global administrative mode of UDLD.
Message Interval	The time period (in seconds) between the transmission of UDLD probe packets.
Timeout Interval	The time period (in seconds) before making a decision that the link is unidirectional.

The following example shows CLI display output for the command after the feature was enabled and nondefault interval values were configured.

```
(Extreme 220) (Routing) #show udld
Admin Mode..................................... Enabled
Message Interval............................... 13
Timeout Interval............................... 31
```

show udld unit/slot/port

This command displays the UDLD settings for the specified unit/slot/port. If the **`all`** keyword is entered, it displays information for all ports.

Format	`show udld {unit/slot/port | all}`
Mode	• User EXEC • Privileged EXEC

Column	Meaning
Port	The identifying port of the interface.
Admin Mode	The administrative mode of UDLD configured on this interface. This is either Enabled or Disabled.
UDLD Mode	The UDLD mode configured on this interface. This is either Normal or Aggressive.
UDLD Status	The status of the link as determined by UDLD. The options are: • Undetermined – UDLD has not collected enough information to determine the state of the port. • Not applicable – UDLD is disabled, either globally or on the port. • Shutdown – UDLD has detected a unidirectional link and shutdown the port. That is, the port is in an errDisabled state. • Bidirectional – UDLD has detected a bidirectional link. • Undetermined (Link Down) – The port would transition into this state when the port link physically goes down due to any reasons other than the port been put into D-Disable mode by the UDLD protocol on the switch.

The following example shows CLI display output for the command.

```
(Extreme 220) #show udld 0/1
Port       Admin Mode   UDLD Mode      UDLD Status
```

```
-----       ----------   -----------    --------------
0/1         Enabled      Normal         Not Applicable
```

The following example shows CLI display output for the command.

```
(Extreme 220) #show udld all
Port        Admin Mode   UDLD Mode      UDLD Status
-----       ----------   -----------    --------------
0/1         Enabled      Normal         Shutdown
0/2         Enabled      Normal         Undetermined
0/3         Enabled      Normal         Bidirectional
0/4         Enabled      Normal         Not Applicable
0/5         Enabled      Normal         Not Applicable
0/6         Enabled      Normal         Not Applicable
0/7         Enabled      Normal         Not Applicable
0/8         Enabled      Normal         Shutdown
0/9         Enabled      Normal         Not Applicable
0/10        Enabled      Normal         Not Applicable
0/11        Enabled      Normal         Not Applicable
0/12        Enabled      Normal         Undetermined
0/13        Enabled      Normal         Bidirectional
0/14        Disabled     Normal         Not Applicable
0/15        Disabled     Normal         Not Applicable
0/16        Disabled     Normal         Not Applicable
0/17        Disabled     Normal         Not Applicable
0/18        Disabled     Normal         Not Applicable
0/19        Disabled     Normal         Not Applicable
0/20        Disabled     Normal         Not Applicable
--More-- or (q)uit
(Extreme 220) #
```

6 Routing Commands

This chapter describes the routing commands available in the 200 Series CLI.

Caution

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.

Address Resolution Protocol Commands

This section describes the commands used to configure *ABR (Area Border Router)* 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.

arp

This command creates an ARP entry. If a virtual router is not specified, the static ARP entry is created in the default router. 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 interface parameter specifies the next hop interface.

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.

Format	`arp` *`ipaddress macaddr`* `interface {`*`unit/slot/port`* `|` `vlan` *`id`*`}`
Mode	Global Config

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. The interface parameter specifies the next hop interface.

Format	`no arp ipaddress macaddr interface unit/slot/port`
Mode	Global Config

ip proxy-arp

This command enables proxy ARP on a router interface or range of interfaces. Without proxy ARP, a device only responds to an ARP request if the target IP address is an address configured on the interface where the ARP request arrived. With proxy ARP, the device may also respond if the target IP address is reachable. The device only responds if all next hops in its route to the destination are through interfaces other than the interface that received the ARP request.

Default	Enabled
Format	`ip proxy-arp`
Mode	Interface Config

no ip proxy-arp

This command disables proxy ARP on a router interface.

Format	`no ip proxy-arp`
Mode	Interface Config

ip local-proxy-arp

Use this command to allow an interface to respond to ARP requests for IP addresses within the subnet and to forward traffic between hosts in the subnet.

Default	Disabled
Format	`ip local-proxy-arp`
Mode	Interface Config

no ip local-proxy-arp

This command resets the local proxy ARP mode on the interface to the default value.

Format	`no ip local-proxy-arp`
Mode	Interface Config

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.

Format	`arp cachesize` *`platform specific integer value`*
Mode	Global Config

no arp cachesize

This command configures the default ARP cache size.

Format	`no arp cachesize`
Mode	Global Config

arp dynamicrenew

This command enables the ARP component to automatically renew 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
Format	`arp dynamicrenew`
Mode	Privileged EXEC

no arp dynamicrenew

This command prevents dynamic ARP entries from renewing when they age out.

Format	`no arp dynamicrenew`
Mode	Privileged EXEC

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.

Format	`arp purge` *`ipaddress`* **`interface`** {*`unit/slot/port`* | `vlan` *`id`*}
Mode	Privileged EXEC

Parameter	Description
`ipaddress`	The IP address to remove from the ARP cache.
`interface`	The interface from which IP addresses will be removed.

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
Format	`arp resptime` *`1-10`*
Mode	Global Config

no arp resptime

This command configures the default ARP request response timeout.

Format	`no arp resptime`
Mode	Global Config

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
Format	`arp retries` *`0-10`*
Mode	Global Config

no arp retries

This command configures the default ARP count of maximum request for retries.

Format	`no arp retries`
Mode	Global Config

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
Format	`arp timeout` *`15-21600`*
Mode	Global Config

no arp timeout

This command configures the default ARP entry ageout time.

Format	`no arp timeout`
Mode	Global Config

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.

Format	`clear arp-cache [gateway]`
Mode	Privileged EXEC

clear arp-switch

Use this command to clear the contents of the switch's Address Resolution Protocol (ARP) table that contains 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.

Format	`clear arp-switch`
Mode	Privileged EXEC

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.

Format	`show arp`
Mode	Privileged EXEC

Column	Meaning
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.
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:

Column	Meaning
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)

show arp brief

This command displays the brief Address Resolution Protocol (ARP) table information .

Format	`show arp brief`
Mode	Privileged EXEC

Column	Meaning
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.

Column	Meaning
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.

show arp switch

This command displays the contents of the switch's Address Resolution Protocol (ARP) table.

Format	`show arp switch`
Mode	Privileged EXEC

Column	Meaning
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's ARP entry.

IP Routing Commands

This section describes the commands used to enable and configure IP routing on the switch.

routing

This command enables IPv4 and IPv6 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
Format	`routing`
Mode	Interface Config

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."

Format	`no routing`
Mode	Interface Config

ip routing

This command enables the IP Router Admin Mode for the master switch.

Format	`ip routing`
Mode	• Global Config • Virtual Router Config

no ip routing

This command disables the IP Router Admin Mode for the master switch.

Format	`no ip routing`
Mode	Global Config

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 on page 515.

Note
The 31-bit subnet mask is only supported on routing interfaces. The feature is not supported on network port and service port interfaces because 200 Series acts as a host, not a router, on these management interfaces.

Format	`ip address` *`ipaddr {subnetmask	/masklen}`*`[secondary]`
Mode	Interface Config

Parameter	Description
`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. Range is 5 to 32 bits.

The following example of the command shows the configuration of the subnet mask with an IP address in the dotted decimal format on interface 0/4/1.

```
(router1) #config
(router1) (Config)#interface 0/4/1
(router1) (Interface 0/4/1)#ip address 192.168.10.1 255.255.255.254
```

The next example of the command shows the configuration of the subnet mask with an IP address in the / notation on interface 0/4/1.

```
(router1) #config
(router1) (Config)#interface 0/4/1
(router1) (Interface 0/4/1)#ip address 192.168.10.1 /31
```

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.

Format	`no ip address [{`*`ipaddr subnetmask`*` [secondary]}]`
Mode	Interface Config

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 (Dynamic Host Configuration Protocol)* 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, use the ip address dhcp client-id configuration command in interface configuration mode.

Default	disabled
Format	`ip address dhcp [client-id]`
Mode	Interface Config

In the following example, DHCPv4 is enabled on interface 0/4/1.

```
(router1) #config
(router1) (Config)#interface 0/4/1
(router1) (Interface 0/4/1)#ip address dhcp
```

no ip address dhcp

The no ip address dhcp command 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.

Format	`no ip address dhcp [client-id]`
Mode	Interface Config

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.

When the system does not have a more specific route to a packet's destination, it sends the packet to the default gateway. The system installs a default IPv4 route with the gateway address as the next hop address. The route preference is 253. A default gateway configured with this command is more preferred than a default gateway learned from a *DHCP* server.

Format	`ip default-gateway` *ipaddr*
Mode	• Global Config • Virtual Router Config

Parameter	Description
ipaddr	The IPv4 address of an attached router.

The following example sets the default gateway to 10.1.1.1.

```
(router1) #config
(router1) (Config)#ip default-gateway 10.1.1.1
```

no ip default-gateway

This command removes the default gateway address from the configuration.

Format	`no ip default-gateway` *ipaddr*
Mode	Interface Config

ip load-sharing

This command configures IP *ECMP (Equal Cost Multi Paths)* load balancing mode.

Default	6
Format	`ip load-sharing` *mode* `{inner | outer}`
Mode	Global Config

Parameter	Description
mode	Configures the load balancing or sharing mode for all EMCP groups. • 1: Based on a hash using the Source IP address of the packet. • 2: Based on a hash using the Destination IP address of the packet. • 3: Based on a hash using the Source and Destination IP addresses of the packet. • 4: Based on a hash using the Source IP address and the Source TCP/UDP Port field of the packet. • 5: Based on a hash using the Destination IP address and the Destination TCP/UDP Port field of the packet. • 6: Based on a hash using the Source and Destination IP address, and the Source and Destination TCP/UDP Port fields of the packet.
inner	Use the inner IP header for tunneled packets.
outer	Use the outer IP header for tunneled packets.

no ip load-sharing

Format	`no ip load-sharing`
Mode	Global Config

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 “administrative distance”) of an individual static 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.

The description parameter allows a description of the route to be entered.

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
Format	`ip route` *`ipaddr subnetmask`* `{` *`nexthopip`* `| Null0 | interface {`*`unit/slot/port`*`|` *`vlan-id`*`}}` *`[preference]`* `[description` *`description`*`]`
Mode	Global Config

Subnetwork 9.0.0.0/24 is a connected subnetwork in global table and subnet 56.6.6.0/24 is reachable via a gateway 9.0.0.2 in the global table.

Subnet 8.0.0.0/24 is a connected subnetwork in virtual router Red.

Now we leak the 2 routes from global route table into the virtual router Red and leak the connected subnet 8.0.0.0/24 from Red to global table.

When leaking connected route in the global routing table to a virtual router, the /32 host route for the leaked host is added in the virtual router instance’s route table.

Also we add a non-leaked static route for 66.6.6.0/24 subnetwork scoped to the domain of virtual router Red.

```
(Router) (Config)#ip routing
(Router) (Config)#ip vrf Red
(Router) (Config)#interface 0/27
```

```
(Router) (Interface 0/27)#routing
(Router) (Interface 0/27)#ip vrf forwarding Red
(Router) (Interface 0/27)#ip address 8.0.0.1 /24
(Router) (Interface 0/27)#interface 0/26
(Router) (Interface 0/26)#routing
(Router) (Interface 0/26)#ip address 9.0.0.1 /24
(Router) (Interface 0/26)#exit
(Router) (Config)#ip route 56.6.6.0 /24 9.0.0.2
Routes leaked from global routing table to VRF's route table are :
(Router) (Config)#ip route vrf Red 9.0.0.2 255.255.255.255 9.0.0.2 0/26
(Router) (Config)#ip route vrf Red 56.6.6.0 255.255.255.0 9.0.0.2 0/26
Route leaked from VRF's route table to global routing table is :
(Router) (Config)#ip route 8.0.0.2 255.255.255.255 0/27
Route (non-leaked) internal to VRF's route table is :
(Router) (Config)#ip route vrf Red 66.6.6.0 255.255.255.0 8.0.0.2
```

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.

Format	`no ip route` *`ipaddr subnetmask [{nexthopip [preference] | Null0}]`*
Mode	Global Config

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
Format	`ip route default` *`nexthopip [preference]`*
Mode	Global Config

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.

Format	`no ip route default` *`[{nexthopip | preference}]`*
Mode	Global Config

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
Format	`ip route distance` *`1-255`*
Mode	Global Config

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.

Format	`no ip route distance`
Mode	Global Config

ip route net-prototype

This command adds net prototype IPv4 routes to the hardware.

Format	`ip route net-prototype` *`prefix/prefix-length nexthopip num-routes`*
Mode	Global Config

Parameter	Description
`prefix/ prefix-length`	The destination network and mask for the route.
`nexthopip`	The next-hop ip address, It must belong to an active routing interface, but it does not need to be resolved.
`num-routes`	The number of routes need to added into hardware starting from the given prefix argument and within the given prefix-length.

no ip route net-prototype

This command deletes all the net prototype IPv4 routes added to the hardware.

Format	`ip route net-prototype` *`prefix/prefix-length nexthopip num-routes`*
Mode	Global Config

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
Format	`ip netdirbcast`
Mode	Interface Config

no ip netdirbcast

This command disables the forwarding of network-directed broadcasts. When disabled, network directed broadcasts are dropped.

Format	`no ip netdirbcast`
Mode	Interface Config

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 (Open Shortest Path First)* 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.)

Note
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 (see mtu on page 279) must take into account the size of the Ethernet header.

For more information about the 200 Series IP MTU, see the Maximum Transmission Unit in 200 Series Application Note (document number 200 Series-AN40X-R).

Default	1500 bytes
Format	`ip mtu` *`68-12270`*
Mode	Interface Config

no ip mtu

This command resets the ip mtu to the default value.

Format	`no ip mtu`
Mode	Interface Config

release dhcp

Use this command to force the DHCPv4 client to release the leased address from the specified interface. The *DHCP* client sends a DHCP Release message telling the DHCP server that it no longer needs the IP address, and that the IP address can be reassigned to another.

Format	`release dhcp {`*`unit/slot/port`* `| vlan` *`id`*`}`
Mode	Privileged EXEC

renew dhcp

Use this command to force the DHCPv4 client to immediately renew an IPv4 address lease on the specified interface.

Note
This command can be used on in-band ports as well as the service or network (out-of-band) port.

Format	`renew dhcp {`*`unit/slot/port`* `| vlan` *`id`*`}`
Mode	Privileged EXEC

renew dhcp network-port

Use this command to renew an IP address on a network port.

Format	`renew dhcp network-port`
Mode	Privileged EXEC

renew dhcp service-port

Use this command to renew an IP address on a service port.

Format	`renew dhcp service-port`
Mode	Privileged EXEC

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
Format	`encapsulation {ethernet | snap}`
Mode	Interface Config

Note
Routed frames are always ethernet encapsulated when a frame is routed to a VLAN.

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.

Format	`show dhcp lease [interface {`*`unit/slot/port`*` | vlan `*`id`*`}]`
Modes	Privileged EXEC

Term	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
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

show ip brief

This command displays the summary information of the IP global configurations, including the *ICMP (Internet Control Message Protocol)* rate limit configuration and the global ICMP Redirect configuration. If no router is specified, information related to the default router is displayed.

Format	`show ip brief`
Modes	• Privileged EXEC • User EXEC

Term	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.

The following example shows CLI display output for the command.

```
(Extreme 220) #show ip brief
Default Time to Live.......................... 64
Routing Mode.................................. Disabled
Maximum Next Hops............................. 4
Maximum Routes................................ 128
ICMP Rate Limit Interval...................... 1000 msec
ICMP Rate Limit Burst Size.................... 100 messages
ICMP Echo Replies............................. Enabled
ICMP Redirects................................ Enabled
```

show ip interface

This command displays all pertinent information about the IP interface. The argument unit/slot/port corresponds to a physical routing interface or VLAN routing interface. The keyword **vlan** is used to specify the VLAN ID of the routing VLAN directly instead of in a unit/slot/port format.

Format	`show ip interface {`*`unit/slot/port`*`|`*`vlan 1-4093`*`|`*`loopback 0-7`*`}`
Modes	• Privileged EXEC • User EXEC

Term	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 ip helper-address (Interface Config) on page 560.
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.
Proxy ARP	Displays whether Proxy ARP is enabled or disabled on the system.
Local Proxy ARP	Displays whether Local Proxy ARP is enabled or disabled on the interface.
Active State	Displays whether the interface is active or inactive. An interface is considered active if its link is up and it is in 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.
Encapsulation Type	The encapsulation type for the specified interface. The types are: Ethernet or SNAP.
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).

Term	Definition
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. See ip address dhcp on page 507.

The following example shows CLI display output for the command.

```
(Extreme 220) #show ip interface 1/0/2
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
Proxy ARP.................................... Enable
Local Proxy ARP.............................. 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
```

In the following example the DHCP client is enabled on a VLAN routing interface.

```
(Extreme 220) (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.................... 0fastpath-0010.1882.160E-vl10
```

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 .

Format	`show ip interface brief`
Modes	• Privileged EXEC • User EXEC

Term	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. • Manual - The address is manually configured.

The following example shows CLI display output for the command.

```
(alpha1) #show ip interface brief
Interface    State  IP Address      IP Mask         Method
----------   -----  --------------- --------------- --------
1/0/17       Up     192.168.75.1    255.255.255.0   DHCP
```

show ip load-sharing

This command displays the currently configured IP *ECMP* load balancing mode.

Format	`show ip load-sharing`
Mode	Privileged Exec

The following example shows CLI display output for the command.

```
(Extreme 220) (Routing) #show ip load-sharing
ip load-sharing 6 inner
```

show ip protocols

This command lists a summary of the configuration and status for each unicast routing protocol. The command lists routing protocols which are configured and enabled. If a protocol is selected on the command line, the display will be limited to that protocol. If no virtual router is specified, the configuration and status for the default router are displayed.

Format	`show ip protocols [bgp|ospf|rip]`
Mode	Privileged EXEC

Parameter	Description
BGP Section:	
Routing Protocol	BGP.

Parameter	Description
Router ID	The router ID configured for BGP.
Local AS Number	The AS number that the local router is in.
BGP Admin Mode	Whether BGP is globally enabled or disabled.
Maximum Paths	The maximum number of next hops in an internal or external BGP route.
Always Compare MED	Whether BGP is configured to compare the MEDs for routes received from peers in different ASs.
Maximum AS Path Length	Limit on the length of AS paths that BGP accepts from its neighbors.
Fast Internal Failover	Whether BGP immediately brings down an iBGP adjacency if the routing table manager reports that the peer address is no longer reachable.
Fast External Failover	Whether BGP immediately brings down an eBGP adjacency if the link to the neighbor goes down.
Distance	The default administrative distance (or route preference) for external, internal, and locally-originated BGP routes. The table that follows lists ranges of neighbor addresses that have been configured to override the default distance with a neighbor-specific distance. If a neighbor's address falls within one of these ranges, routes from that neighbor are assigned the configured distance. If a prefix list is configured, then the distance is only assigned to prefixes from the neighbor that are permitted by the prefix list.
Redistribution	A table showing information for each source protocol (connected, static, rip, and ospf). For each of these sources the distribution list and route-map are shown, as well as the configured metric. Fields which are not configured are left blank. For ospf, an additional line shows the configured ospf match parameters.
Prefix List In	The global prefix list used to filter inbound routes from all neighbors.
Prefix List Out	The global prefix list used to filter outbound routes to all neighbors.
Networks Originated	The set of networks originated through a network command. Those networks that are actually advertised to neighbors are marked "active."
Neighbors	A list of configured neighbors and the inbound and outbound policies configured for each.
OSPFv2 Section:	
Routing Protocol	OSPFv2.
Router ID	The router ID configured for OSPFv2.
OSPF Admin Mode	Whether OSPF is enabled or disabled globally.
Maximum Paths	The maximum number of next hops in an OSPF route.

Parameter	Description
Routing for Networks	The address ranges configured with an OSPF network command.
Distance	The administrative distance (or “route preference”) for intra-area, inter-area, and external routes.
Default Route Advertise	Whether OSPF is configured to originate a default route.
Always	Whether default advertisement depends on having a default route in the common routing table.
Metric	The metric configured to be advertised with the default route.
Metric Type	The metric type for the default route.
Redist Source	A type of routes that OSPF is redistributing.
Metric	The metric to advertise for redistributed routes of this type.
Metric Type	The metric type to advertise for redistributed routes of this type.
Subnets	Whether OSPF redistributes subnets of classful addresses, or only classful prefixes.
Dist List	A distribute list used to filter routes of this type. Only routes that pass the distribute list are redistributed.
Number of Active Areas	The number of OSPF areas with at least one interface running on this router. Also broken down by area type.
ABR Status	Whether the router is currently an area border router. A router is an area border router if it has interfaces that are up in more than one area.
ASBR Status	Whether the router is an autonomous system boundary router. The router is an ASBR if it is redistributing any routes or originating a default route.
RIP Section	
RIP Admin Mode	Whether *RIP (Routing Information Protocol)* is globally enabled.
Split Horizon Mode	Whether RIP advertises routes on the interface where they were received.
Default Metric	The metric assigned to redistributed routes.
Default Route Advertise	Whether this router is originating a default route.
Distance	The administrative distance for RIP routes.
Redistribution	A table showing information for each source protocol (connected, static, bgp, and ospf). For each of these source the distribution list and metric are shown. Fields which are not configured are left blank. For ospf, configured ospf match parameters are also shown.
Interface	The interfaces where RIP is enabled and the version sent and accepted on each interface.

The following example shows CLI display output for the command.

```
(Router) #show ip protocols
Routing Protocol..................... BGP
Router ID............................ 6.6.6.6
Local AS Number...................... 65001
BGP Admin Mode....................... Enable
Maximum Paths........................ Internal 32, External 32
Always compare MED ..................... FALSE
Maximum AS Path Length ................. 75
Fast Internal Failover ..................... Enable
Fast External Failover ..................... Enable
Distance............................. Ext 20 Int 200 Local 200
  Address         Wildcard        Distance    Pfx List
  -------         --------        --------    --------
  172.20.0.0      0.0.255.255           40        None
  172.21.0.0      0.0.255.255           45           1
Prefix List In....................... PfxList1
Prefix List Out...................... None
Redistributing:
Source        Metric  Dist List               Route Map
--------- ----------  ---------------------- ---------------------------
connected             connected_list
static         32120                         static_routemap
rip            30000                         rip_routemap
ospf                                         ospf_map
  ospf match: int ext1 nssa-ext2
   Networks Originated:
     10.1.1.0 255.255.255.0 (active)
     20.1.1.0 255.255.255.0
Neighbors:
172.20.1.100
   Filter List In..................... 1
   Filter List Out.................... 2
   Prefix List In..................... PfxList2
   Prefix List Out.................... PfxList3
   Route Map In....................... rmapUp
   Route Map Out...................... rmapDown
172.20.5.1
   Prefix List Out.................... PfxList12
Routing Protocol..................... OSPFv2
Router ID............................ 6.6.6.6
OSPF Admin Mode...................... Enable
Maximum Paths........................ 32
Routing for Networks................. 172.24.0.0 0.0.255.255 area 0
                                      10.0.0.0 0.255.255.255 area 1
                                      192.168.75.0 0.0.0.255 area 2
Distance............................. Intra 110 Inter 110 Ext 110
Default Route Advertise.............. Disabled
Always............................... FALSE
Metric............................... Not configured
Metric Type.......................... External Type 2
Redist
Source      Metric       Metric Type     Subnets    Dist List
---------  -------       -----------     -------    ---------
static     default                2         Yes         None
connected       10                2         Yes            1
Number of Active Areas............... 3 (3 normal, 0 stub, 0 nssa)
ABR Status........................... Yes
ASBR Status.......................... Yes
Routing Protocol..................... RIP
RIP Admin Mode....................... Enable
Split Horizon Mode................... Simple
Default Metric....................... Not configured
```

```
Default Route Advertise..................... Disable
Distance.................................... 120
Redistribution:
Source    Metric Dist List Match
--------- ------ --------- ---------------------------------------
connected      6
static        10        15
ospf                    20 int ext1 ext2 nssa-ext1
Interface              Send        Recv
---------              ----        ----
0/25                   RIPv2       RIPv2
```

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 protocol can be connected, ospf, rip, or static, or bgp. Use the all parameter to display all routes including best and nonbest routes. If you do not use the all parameter, the command displays only the best route.

Note
If you use the **connected** keyword for *protocol*, the **all** option is not available because there are no best or nonbest connected routes.

Note
If you use the **static** keyword for *protocol*, the **description** option is also available, for example: show ip route ip-address static description. This command shows the description configured with the specified static route(s).

Format	`show ip route` *ip-address [protocol]* | {*ip-address mask* `[longer-prefixes]` *[protocol]* | *protocol*} `[all]` | `all}]`
Modes	• Privileged EXEC • User EXEC

Term	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:

Term	Definition
Code	The codes for the routing protocols that created the routes.

Term	Definition
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.
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:Minutes: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/*RIP*. Reject routes are supported in both OSPFv2 and *OSPFv3 (Open Shortest Path First version 3)*.

The following example shows CLI display output for the command.

```
(Extreme 220) (Routing) #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        L-Leaked
Route K - Kernel P - Net Prototype
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
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
```

```
C 11.11.11.0/24 [0/1] directly connected, 0/11
S 10.3.2.0/24 [1/0] via 1.1.1.2, 0/11
```

The following example shows 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
       L-Leaked Route K - Kernel P - Net Prototype
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
```

The following shows an example of output that displays leaked routes.

Subnetwork 9.0.0.0/24 is a connected subnetwork in global table and subnet 56.6.6.0/24 is reachable via a gateway 9.0.0.2 in the global table. These two routes leak into the virtual router Red and leak the connected subnet 8.0.0.0/24 from Red to global table.

When leaking connected route in the global routing table to a virtual router, the /32 host route for the leaked host is added in the virtual router instance's route table. Leaking of non /32 connected routes into the virtual router table from global routing table is not supported.

This enables the nodes in subnet 8.0.0.0/24 to access shared services via the global routing table. Also we add a non-leaked static route for 66.6.6.0/24 subnetwork scoped to the domain of virtual router Red.

```
(Router) (Config)#ip route vrf Red 9.0.0.2 255.255.255.255 9.0.0.2 0/26
(Router) (Config)#ip route vrf Red 56.6.6.0 255.255.255.0 9.0.0.2 0/26
(Router) (Config)#ip route vrf Red 66.6.6.0 255.255.255.0 8.0.0.2
(Router) (Config)#ip route 8.0.0.0 255.255.255.0 0/27
(Router) #show ip route vrf Red
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
        L - Leaked Route K - Kernel P - Net Prototype
C      8.0.0.0/24 [0/1] directly connected,   0/27
S L    9.0.0.2/32 [1/1] directly connected,   0/26
S L    56.6.6.0/24 [1/1] via 9.0.0.2,   02d:22h:15m,  0/26
S      66.6.6.0/24 [1/1] via 8.0.0.2,   01d:22h:15m,  0/27
(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
    L - Leaked Route
C      9.0.0.0/24 [0/1] directly connected,   0/26
S L    8.0.0.0/24 [1/1] directly connected,   0/27
The following shows an example of the output that displays with a hardware failure.
(Router) (Config)#interface 0/1
(Router) (Interface 0/1)#routing
(Router) (Interface 0/1)#ip address 9.0.0.1 255.255.255.0
(Router) (Interface 0/1)#exit
(Router) (Config)#ip route net-prototype 56.6.6.0/24 9.0.0.2 1
(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

```
       S U - Unnumbered Peer, L - Leaked Route, K - Kernel     P - Net Prototype
C      9.0.0.0/24 [0/0] directly connected,   0/1
P      56.6.6.0/24 [1/1] via 9.0.0.2,   01d:22h:15m,  0/1  hw-failure
```

show ip route ecmp-groups

This command reports all current *ECMP* groups in the IPv4 routing table. An ECMP group is a set of two or more next hops used in one or more routes. The groups are numbered arbitrarily from 1 to n. The output indicates the number of next hops in the group and the number of routes that use the set of next hops. The output lists the IPv4 address and outgoing interface of each next hop in each group.

Format	`show ip route ecmp-groups`
Mode	Privileged EXEC

The following example shows CLI display output for the command.

```
(router) #show ip route ecmp-groups
ECMP Group 1 with 2 next hops (used by 1 route)
  172.20.33.100 on interface 2/33
  172.20.34.100 on interface 2/34
ECMP Group 2 with 3 next hops (used by 1 route)
  172.20.32.100 on interface 2/32
  172.20.33.100 on interface 2/33
  172.20.34.100 on interface 2/34
ECMP Group 3 with 4 next hops (used by 1 route)
  172.20.31.100 on interface 2/31
  172.20.32.100 on interface 2/32
  172.20.33.100 on interface 2/33
  172.20.34.100 on interface 2/34
```

show ip route hw-failure

Use this command to display the routes that failed to be added to the hardware due to hash errors or a table full condition.

Format	`show ip route hw-failure`
Mode	Privileged EXEC

The following example displays the command output.

```
(Extreme 220) (Config) #ip route net-prototype 66.6.6.0/24 9.0.0.2 4
(Extreme 220) (Routing) #show ip route connected
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
       S U - Unnumbered Peer, L - Leaked Route, K - Kernel
    P - Net Prototype
C      9.0.0.0/24 [0/0] directly connected,   0/1
C      8.0.0.0/24 [0/0] directly connected,   0/2
(Extreme 220) (Routing) #show ip route hw-failure
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
       S U - Unnumbered Peer, L - Leaked Route, K - Kernel
    P - Net Prototype
P      66.6.6.0/24 [1/1] via 9.0.0.2,   01d:22h:15m,  0/1  hw-failure
P      66.6.7.0/24 [1/1] via 9.0.0.2,   01d:22h:15m,  0/1  hw-failure
P      66.6.8.0/24 [1/1] via 9.0.0.2,   01d:22h:15m,  0/1  hw-failure
P      66.6.9.0/24 [1/1] via 9.0.0.2,   01d:22h:15m,  0/1  hw-failure
```

show ip route net-prototype

This command displays the net-prototype routes. The net-prototype routes are displayed with a P.

Format	`show ip route net-prototype`
Modes	Privileged EXEC

```
(Extreme 220) (Routing) #show ip route net-prototype
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
       S U - Unnumbered Peer, L - Leaked Route, K - Kernel
       P - Net Prototype
P      56.6.6.0/24 [1/1] via 9.0.0.2,   01d:22h:15m,  0/1
P      56.6.7.0/24 [1/1] via 9.0.0.2,   01d:22h:15m,  0/1
```

show ip route summary

This command displays a summary of the state of the routing table. 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.

Format	`show ip route summary [all]`
Modes	• Privileged EXEC • User EXEC

Term	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 the BGP protocol.
External	The number of external BGP routes.

Term	Definition
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. The value in parentheses indicates the highest count of unique best routes since counters were last cleared.
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.
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 route adds that failed because none of the route's next hops were on a local 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.
Hardware Failed Route Adds	The number of routes failed be inserted into the hardware due to hash error or a table full condition.

Term	Definition
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 (High)	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. The value in parentheses indicates the highest count of unique next hops since counters were last cleared.
Next Hop Groups (High)	The current number of next hop groups in use by one or more routes. Each next hop group includes one or more next hops. The value in parentheses indicates 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.

The following example shows CLI display output for the command.

```
(Extreme 220) (Routing) #show ip route summary
Connected Routes.............................. 7
Static Routes................................. 1
RIP Routes.................................... 20
BGP Routes.................................... 10
  External.................................... 0
  Internal.................................... 10
  Local....................................... 0
OSPF Routes................................... 1004
  Intra Area Routes........................... 4
  Inter Area Routes........................... 1000
  External Type-1 Routes...................... 0
  External Type-2 Routes...................... 0
Reject Routes................................. 0
Net Prototype Routes.......................... 10004
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
Hardware Failed Route Adds......................  4
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
```

clear ip route counters

The command resets to zero the IPv4 routing table counters reported in the command show ip route summary on page 526. 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.

Format	`clear ip route counters`
Mode	Privileged EXEC

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

Format	`show ip route preferences`
Modes	• Privileged EXEC • User EXEC

Term	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.
BGP Internal	The BGP internal route preference value.

Term	Definition
BGP Local	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.

The following example shows 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
```

show ip stats

This command displays IP statistical information.

Format	`show ip stats`
Modes	• Privileged EXEC • User EXEC

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.

Format	`show routing heap summary`
Mode	Privileged EXEC

Parameter	Description
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.

Parameter	Description
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.

The following example shows 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
```

Routing Policy Commands

ip policy route-map

Use this command to identify a route map to use for policy-based routing on an interface specified by route-map-name. Policy-based routing is configured on the interface that receives the packets, not on the interface from which the packets are sent.

When a route-map applied on the interface is changed, that is, if new statements are added to route-map or match/set terms are added/removed from route-map statement, and also if route-map that is applied on an interface is removed, route-map needs to be removed from interface and added back again in order to have changed route-map configuration to be effective.

Note
Route-map and DiffServ cannot work on the same interface.

Format	`ip policy route-map` *`route-map-name`*
Mode	Interface Config

The following is an example of this command.

```
(Extreme 220) (Config) #interface 1/0/1
(Extreme 220) (Interface 1/0/1)#
 (Extreme 220) (Switching) (Interface 1/0/1)# #ip policy route-map equal-access
In order to disable policy based routing from an interface, use no form of this command
no ip policy route-map route-map-name
```

ip prefix-list

To create a prefix list or add a prefix list entry, use the ip prefix-list command in Global Configuration mode. Prefix lists allow matching of route prefixes with those specified in the prefix list. Each prefix list includes of a sequence of prefix list entries ordered by their sequence numbers. A router sequentially

examines each prefix list entry to determine if the route's prefix matches that of the entry. An empty or nonexistent prefix list permits all prefixes. An implicit deny is assume if a given prefix does not match any entries of a prefix list. Once a match or deny occurs the router does not go through the rest of the list. A prefix list may be used within a route map to match a route's prefix using the `match ip address` command (see match ip address on page 537).

Up to 128 prefix lists may be configured. The maximum number of statements allowed in prefix list is 64.

Default	No prefix lists are configured by default. When neither the ge nor the **le** option is configured, the destination prefix must match the network/length exactly. If the **ge** option is configured without the **le** option, any prefix with a network mask greater than or equal to the ge value is considered a match. Similarly, if the **le** option is configured without the **ge** option, a prefix with a network mask less than or equal to the le value is considered a match.
Format	`ip prefix-list` *`list-name`* `{[`*`seq number`*`] {permit | deny}` *`network/length`* `[`**`ge`** `length] [`**`le`** `length] |` **`renumber`** *`renumber-interval first-statement-number`*`}`
Mode	Global Configuration

Parameter	Description
`list-name`	The text name of the prefix list. Up to 32 characters.
`seq number`	(Optional) The sequence number for this prefix list statement. Prefix list statements are ordered from lowest sequence number to highest and applied in that order. If you do not specify a sequence number, the system will automatically select a sequence number five larger than the last sequence number in the list. Two statements may not be configured with the same sequence number. The value ranges from 1 to 4,294,967,294.
`permit`	Permit routes whose destination prefix matches the statement.
`deny`	Deny routes whose destination prefix matches the statement.
`network/ length`	Specifies the match criteria for routes being compared to the prefix list statement. The network can be any valid IP prefix. The length is any IPv4 prefix length from 0 to 32.
`ge` *`length`*	(Optional) If this option is configured, then a prefix is only considered a match if its network mask length is greater than or equal to this value. This value must be longer than the network length and less than or equal to 32.
`le` *`length`*	(Optional) If this option is configured, then a prefix is only considered a match if its network mask length is less than or equal to this value. This value must be longer than the ge length and less than or equal to 32.
`renumber`	(Optional) Provides the option to renumber the sequence numbers of the IP prefix list statements with a given interval starting from a particular sequence number. The valid range for renumber-interval is 1–100, and the valid range for first-statement-number is 1–1000.

The following example configures a prefix list that allows routes with one of two specific destination prefixes, 172.20.0.0/16 and 192.168.1.0/24:

```
(Extreme 220) (Routing)(config)# ip prefix-list apple seq 10 permit 172.20.0.0/16
(Extreme 220) (Routing)(config)# ip prefix-list apple seq 20 permit 192.168.10/24
```

The following example disallows only the default route.

```
(Extreme 220) (Routing)(config)# ip prefix-list orange deny 0.0.0.0/0
(Extreme 220) (Routing)(config)# ip prefix-list orange permit 0.0.0.0/0 ge 1
```

no ip prefix-list

To delete a prefix list or a statement in a prefix list, use the no form of this command. The command no ip prefix-list *list-name* deletes the entire prefix list. To remove an individual statement from a prefix list, you must specify the statement exactly, with all its options.

Format	`no ip prefix-list` *`list-name`* `[`*`seq number`*`] { permit | deny }` *`network/length`* `[`**`ge`** *`length`*`] [`**`le`** *`length`*`]`
Mode	Global Configuration

ip prefix-list description

To apply a text description to a prefix list, use the ip prefix-list description command in Global Configuration mode.

Default	No description is configured by default.
Format	`ip prefix-list` *`list-name`* **`description`** *`text`*
Mode	Global Configuration

Parameter	Description
`list-name`	The text name of the prefix list.
`text`	Text description of the prefix list. Up to 80 characters.

no ip prefix-list description

To remove the text description, use the no form of this command.

Format	`no ip prefix-list` *`list-name`* `description`
Mode	Global Configuration

ipv6 prefix-list

Use this command to create IPv6 prefix lists. An IPv6 prefix list can contain only ipv6 addresses. Prefix lists allow matching of route prefixes with those specified in the prefix list. Each prefix list includes of a sequence of prefix list entries ordered by their sequence numbers. A router sequentially examines each prefix list entry to determine if the route's prefix matches that of the entry. For IPv6 routes, only IPv6 prefix lists are matched. An empty or nonexistent prefix list permits all prefixes. An implicit deny is assumed if a given prefix does not match any entries of a prefix list. Once a match or deny occurs the router does not go through the rest of the list. An IPv6 prefix list may be used within a route map to match a route's prefix using the `match ipv6 address` command. A route map may contain both IPv4 and IPv4 prefix lists. If a route being matched is an IPv6 route, only the IPv6 prefix lists are matched.

Up to 128 prefix lists may be configured. The maximum number of statements allowed in prefix list is 64. These numbers indicate only IPv6 prefix lists. IPv4 prefix lists may be configured in appropriate numbers independently.

Default	No prefix lists are configured by default. When neither the ge nor the **le** option is configured, the destination prefix must match the network/length exactly. If the **ge** option is configured without the **le** option, any prefix with a network mask greater than or equal to the ge value is considered a match. Similarly, if the **le** option is configured without the **ge** option, a prefix with a network mask less than or equal to the le value is considered a match.
Format	`ipv6 prefix-list` *`list-name`* `[seq` *`seq-number`*`] { {permit/deny}` *`ipv6-prefix/prefix-length`* `[ge` *`ge-value`*`] [le` *`le-value`*`] | description` *`text`* `| renumber` *`renumber-interval first-statement-number`*`}`
Mode	Global Configuration

Parameter	Description
`list-name`	The text name of the prefix list. Up to 32 characters.
seq number	(Optional) The sequence number for this prefix list statement. Prefix list statements are ordered from lowest sequence number to highest and applied in that order. If you do not specify a sequence number, the system will automatically select a sequence number five larger than the last sequence number in the list. Two statements may not be configured with the same sequence number. The value ranges from 1 to 4,294,967,294.
permit	Permit routes whose destination prefix matches the statement.
deny	Deny routes whose destination prefix matches the statement.
ipv6-prefix/ prefix-length	Specifies the match criteria for routes being compared to the prefix list statement. The ipv6-prefix can be any valid IPv6 prefix where the address is specified in hexadecimal using 16-bit values between colons. The prefix-length is the The length of the IPv6 prefix, given as a decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
ge length	(Optional) If this option is configured, specifies a prefix length greater than or equal to the ipv6-prefix/prefix-length. It is the lowest value of a range of the length.
le length	(Optional) If this option is configured, specifies a prefix length less than or equal to the ipv6-prefix/prefix-length. It is the highest value of a range of the length.
Description	A description of the prefix list. It can be up to 80 characters in length.
renumber	(Optional) Provides the option to renumber the sequence numbers of the IPv6 prefix list statements with a given interval starting from a particular sequence number.

The following example configures a prefix list that allows routes with one of two specific destination prefixes, 2001::/64 and 5F00::/48:

```
(R1)(config)# ipv6 prefix-list apple seq 10 permit 2001::/64
(R1)(config)# ipv6 prefix-list apple seq 20 permit 5F00::/48
```

no ipv6 prefix-list

Use this command to deletes either the entire prefix list or an individual statement from a prefix list.

Format	`no ipv6 prefix-list list-name`
Mode	Global Configuration

Note
The description must be removed using no ip prefix-list description before using this command to delete an IPv6 Prefix List.

route-map

To create a route map and enter Route Map Configuration mode, use the route-map command in Global Configuration mode. One use of a route map is to limit the redistribution of routes to a specified range of route prefixes. The redistribution command specifies a route map which refers to a prefix list. The prefix list identifies the prefixes that may be redistributed. 200 Series accepts up to 64 route maps.

Default	No route maps are configured by default. If no permit or deny tag is given, permit is the default.
Format	`route-map map-tag [permit|deny] [sequence-number]`
Mode	Global Configuration

Parameter	Description
map-tag	Text name of the route map. Route maps with the same name are grouped together in order of their sequence numbers. A route map name may be up to 32 characters long.
permit	(Optional) Permit routes that match all of the match conditions in the route map.
deny	(Optional) Deny routes that match all of the match conditions in the route map.
sequence-number	(Optional) An integer used to order the set of route maps with the same name. Route maps are ordered from lowest to greatest sequence number, with lower sequence numbers being considered first. If no sequence number is specified, the system assigns a value ten greater than the last statement in the route map. The range is 0 to 65,535.

In the following example, BGP is configured to redistribute the all prefixes within 172.20.0.0 and reject all others.

```
(Extreme 220) (Config)# ip prefix-list redist-pl permit 172.20.0.0/16 le 32
(Extreme 220) (Config)# route-map redist-rm permit
(Extreme 220)(config-route-map)# match ip address prefix-list redist-pl
(Extreme 220)(config-route-map)# exit
(Extreme 220) (Config) router bgp 1
(Extreme 220)(Config-router) redistribute ospf route-map redist-rm
```

no route-map

To delete a route map or one of its statements, use the no form of this command.

Format	`no route-map map-tag [permit|deny] [sequence-number]`
Mode	Global Configuration

match as-path

This route map match term matches *BGP (Border Gateway Protocol)* autonomous system paths against an AS path access list. If you enter a new match as-path term in a route map statement that already has a match as-path term, the AS path list numbers in the new term are added to the existing match term, up to the maximum number of lists in a term. A route is considered a match if it matches any one or more of the AS path access lists the match term refers to.

Format	`match as-path` *`as-path-list-number`*
Mode	Route Map Configuration

Parameter	Description
`as-path-list-number`	An integer from 1 to 500 identifying the AS path access list to use as match criteria.

no match as-path

This command deletes the match as-path term that matches BGP autonomous system paths against an AS path access list.

Format	`no match as-path` *`as-path-list-number`*
Mode	Route Map Configuration

match community

To configure a route map to match based on a *BGP* community list, use the match community command in Route Map Configuration mode. If the community list returns a permit action, the route is considered a match. If the match statement refers to a community list that is not configured, no routes are considered to match the statement.

Format	`match community` *`community-list`* `[`*`community-list...`*`] [exact-match]`
Mode	Route Map Configuration

Parameter	Description
`community-list`	The name of a standard community list. Up to eight names may be included in a single match term.
`exact-match`	(Optional) When this option is given, a route is only considered a match if the set of communities on the route is an exact match for the set of communities in one of the statements in the community list.

no match community

To delete a match term from a route map, use the no form of this command. The command no match community list exact-match removes the match statement from the route map. (It does not simply

remove the exact-match option.) The command no match community removes the match term and all its community lists.

Format	`no match community` *`community-list`* `[`*`community-list...`*`] [exact-match]`
Mode	Route Map Configuration

match ip address

To configure a route map to match based on a destination prefix, use the match ip address command in Route Map Configuration mode. If you specify multiple prefix lists in one statement, then a match occurs if a prefix matches any one of the prefix lists. If you configure a match ip address statement within a route map section that already has a match ip address statement, the new prefix lists are added to the existing set of prefix lists, and a match occurs if any prefix list in the combined set matches the prefix.

Default	No match criteria are defined by default.
Format	`match ip address prefix-list` *`prefix-list-name`* `[`*`prefix-list-name...`*`]`
Mode	Route Map Configuration

Parameter	Description
`prefix-list-name`	The name of a prefix list used to identify the set of matching routes. Up to eight prefix lists may be specified.

no match ip address

To delete a match statement from a route map, use the no form of this command.

Format	`no match ip address [prefix-list` *`prefix-list-name`* `[`*`prefix-list-name...`*`]]`
Mode	Route Map Configuration

match ip address access-list-number | access-list-name

Use this command to configure a route map in order to match based on the match criteria configured in an IP access-list. Note that an IP *ACL (Access Control List)* must be configured before it is linked to a route-map. Actions present in an IP ACL configuration are applied with other actions involved in route-map. If an IP ACL referenced by a route-map is removed or rules are added or deleted from that ACL, the configuration is rejected.

If there are a list of IP access-lists specified in this command and the packet matches at least one of these access-list match criteria, the corresponding set of actions in route-map are applied to packet.

If there are duplicate IP access-list numbers/names in this command, the duplicate configuration is ignored.

Default	No match criteria are defined by default.
Format	`match ip address` *`access-list-number	access-list-name [...access-list-number| name]`*
Mode	Route Map Configuration

Parameter	Description
`access-list-number`	The access-list number that identifies an access-list configured through access-list CLI configuration commands. This number is 1 to 99 for standard access list number. This number is 100 to 199 for extended access list number.
`access-list-name`	The access-list name that identifies named IP ACLs. Access-list name can be up to 31 characters in length. A maximum of 16 ACLs can be specified in this 'match' clause.

The following sequence shows creating a route-map with "match" clause on ACL number and applying that route-map on an interface.

```
(Extreme 220) (Config) #access-list 1 permit ip 10.1.0.0 0.0.255.255
(Extreme 220) (Config) #access-list 2 permit ip 10.2.0.0 0.0.255.255
(Extreme 220) (Config) #route-map equal-access permit 10
(Extreme 220) (config-route-map)#match ip address 1
(Extreme 220) (config-route-map)#set ip default next-hop 192.168.6.6
(Extreme 220) (config-route-map)#route-map equal-access permit 20
(Extreme 220) (config-route-map)#match ip address 2
(Extreme 220) (config-route-map)#set ip default next-hop 172.16.7.7
(Extreme 220) (Config) #interface 1/0/1
(Extreme 220) (Interface 1/0/1)#ip address 10.1.1.1 255.255.255.0
(Extreme 220) (Interface 1/0/1)#ip policy route-map equal-access
(Extreme 220) (Config) #interface 1/0/2
(Extreme 220) (Interface 1/0/2)#ip address 192.168.6.5 255.255.255.0
(Extreme 220) (Config) #interface 1/0/3
(Extreme 220) (Interface 1/0/3)#ip address 172.16.7.6 255.255.255.0
The ip policy route-map equal-access command is applied to interface 1/0/1. All packets
coming inside 1/0/1 are policy-routed.
Sequence number 10 in route map equal-access is used to match all packets sourced from any
host in subnet 10.1.0.0. If there is a match, and if the router has no explicit route for
the packet's destination, it is sent to next-hop address 192.168.6.6 .
Sequence number 20 in route map equal-access is used to match all packets sourced from any
host in subnet 10.2.0.0. If there is a match, and if the router has no explicit route for
the packet's destination, it is sent to next-hop address 172.16.7.7.
Rest all packets are forwarded as per normal L3 destination-based routing.
```

This example illustrates the scenario where IP ACL referenced by a route-map is removed or rules are added or deleted from that ACL, this is how configuration is rejected:

```
(Extreme 220) (Routing) #show ip access-lists
Current number of ACLs: 9  Maximum number of ACLs: 100
ACL ID/Name                     Rules  Direction  Interface(s)      VLAN(s)
------------------------------  -----  ---------  ----------------  ----------
1                               1
2                               1
3                               1
4                               1
5                               1
madan                           1
(Extreme 220) (Routing) #show mac access-lists
```

```
Current number of all ACLs: 9  Maximum number of all ACLs: 100
MAC ACL Name                     Rules  Direction  Interface(s)       VLAN(s)
-------------------------------  -----  ---------  ----------------  ----------
madan                            1
mohan                            1
goud                             1
(Extreme 220) (Routing) #
(Extreme 220) (Routing) #
(Extreme 220) (Routing) #configure
(Extreme 220) (Config) #route-map madan
(Extreme 220) (route-map)#match ip address 1 2 3 4 5 madan
(Extreme 220) (route-map)#match mac-list madan mohan goud
(Extreme 220) (route-map)#exit
(Extreme 220) (Config) #exit
(Extreme 220) (Routing) #show route-map
route-map madan permit 10
     Match clauses:
       ip address (access-lists) : 1 2 3 4 5 madan
       mac-list (access-lists) : madan mohan goud
     Set clauses:
(Extreme 220) (Config) #access-list 2 permit every
Request denied. Another application using this ACL restricts the number of rules allowed.
(Extreme 220) (Config) #ip access-list madan
(Extreme 220) (Config-ipv4-acl)#permit udp any any
Request denied. Another application using this ACL restricts the number of rules allowed.
```

no match ip address

To delete a match statement from a route map, use the no form of this command.

Format	`no match ip address [access-list-number | access-list-name]`
Mode	Route Map Configuration

match ipv6 address

Use this command to configure a route map to match based on a destination prefix. prefix-list *prefix-list-name* identifies the name of an IPv6 prefix list used to identify the set of matching routes. Up to eight prefix lists may be specified. If multiple prefix lists are specified, a match occurs if a prefix matches any one of the prefix lists. If you configure a match ipv6 address statement within a route map section that already has a match ipv6 address statement, the new prefix lists are added to the existing set of prefix lists, and a match occurs if any prefix list in the combined set matches the prefix.

Default	No match criteria are defined by default.
Format	`match ipv6 address prefix-list prefix-list-name [prefix-list-name...]`
Mode	Route Map Configuration

In the following example, IPv6 addresses specified by the prefix list apple are matched through the route map abc.

```
Router(config)# route-map abc
Router(config-route-map)# match ipv6 address prefix-list apple
```

no match ipv6 address

To delete a match statement from a route map, use the no form of this command.

Format	`no match ipv6 address prefix-list prefix-list-name [prefix-list-name...]]`
Mode	Route Map Configuration

match length

Use this command to configure a route map to match based on the Layer 3 packet length between specified minimum and maximum values. min specifies the packet's minimum Layer 3 length, inclusive, allowed for a match. max specifies the packet's maximum Layer 3 length, inclusive, allowed for a match. Each route-map statement can contain one 'match' statement on packet length range.

Default	No match criteria are defined by default.
Format	`match length min max`
Mode	Route Map Configuration

The following shows an example of the command.

```
(Extreme 220) (config-route-map)# match length 64 1500
```

no match length

Use this command to delete a match statement from a route map.

Format	`no match length`
Mode	Route Map Configuration

match mac-list

Use this command to configure a route map in order to match based on the match criteria configured in an MAC access-list.

A MAC *ACL* is configured before it is linked to a route-map. Actions present in MAC ACL configuration are applied with other actions involved in route-map. When a MAC ACL referenced by a route-map is removed, the route-map rule is also removed and the corresponding rule is not effective. When a MAC ACL referenced by a route-map is removed or rules are added or deleted from that ACL, the configuration is rejected.

Default	No match criteria are defined by default.
Format	`match mac-list mac-list-name [mac-list-name]`
Mode	Route Map Configuration

Parameter	Description
mac-list-name	The mac-list name that identifies MAC ACLs. MAC Access-list name can be up to 31 characters in length.

The following is an example of the command.

```
(Extreme 220) (config-route-map)# match mac-list MacList1
Example 2:
This example illustrates the scenario where MAC ACL referenced by a route-map is removed
or rules are added or deleted from that ACL, this is how configuration is rejected:
(Extreme 220) (Routing) #show mac access-lists
Current number of all ACLs: 9  Maximum number of all ACLs: 100
MAC ACL Name                     Rules  Direction  Interface(s)       VLAN(s)
-------------------------------  -----  ---------  ----------------  ----------
madan                            1
mohan                            1
goud                             1
(Extreme 220) (Routing) #
(Extreme 220) (Routing) #
(Extreme 220) (Routing) #configure
(Extreme 220) (Config) #route-map madan
(Extreme 220) (route-map)#match mac-list madan mohan goud
(Extreme 220) (route-map)#exit
(Extreme 220) (Config) #exit
(Extreme 220) (Routing) #show route-map
route-map madan permit 10
     Match clauses:
       mac-list (access-lists) : madan mohan goud
     Set clauses:
(Extreme 220) (Config) #mac access-list extended madan
(Extreme 220) (Config-mac-access-list)#permit 00:00:00:00:00:01 ff:ff:ff:ff:ff:ff any
Request denied. Another application using this ACL restricts the number of rules allowed.
```

no match mac-list

To delete a match statement from a route map, use the no form of this command.

Format	`no match mac-list […mac-list-name]`
Mode	Route Map Configuration

set as-path

To prepend one or more AS numbers to the AS path in a BGP route, use the set as-path command in Route Map Configuration mode. This command is normally used to insert one or more instances of the local AS number at the beginning of the AS_PATH attribute of a BGP route. Doing so increases the AS path length of the route. The AS path length has a strong influence on BGP route selection. Changing the AS path length can influence route selection on the local router or on routers to which the route is advertised.

When prepending an inbound route, if the first segment in the AS_PATH of the received route is an AS_SEQUENCE, as-path-string is inserted at the beginning of the sequence. If the first segment is an AS_SET, as-path-string is added as a new segment with type AS_SEQUENCE at the beginning of the AS path. When prepending an outbound route to an external peer, as-path-string follows the local AS number, which is always the first ASN.

Format	`set as-path prepend` *`as-path-string`*
Mode	Route Map Configuration

Parameter	Description
`as-path-string`	A list of AS path numbers to insert at the beginning of the AS_PATH attribute of matching BGP routes. To prepend more than one AS number, separate the ASNs with a space and enclose the string in quotes. Up to ten AS numbers may be prepended.

The following example prepends three instances an external peer's AS number to paths received from that peer, making routes learned from this peer less likely to be chosen as the best path.

```
(Extreme 220) (Routing)# config
(Extreme 220) (Routing)# route-map ppAsPath
(Extreme 220) (Routing)# set as-path prepend "2 2 2"
(Extreme 220) (Routing)# exit
(Extreme 220) (Routing)# router bgp 1
(Extreme 220) (Routing)# neighbor 172.20.1.2 remote-as 2
(Extreme 220) (Routing)# neighbor 172.20.1.2 route-map ppAsPath in
```

no set as-path

To remove a set command from a route map, use the no form of this command.

Format	`no set as-path prepend` *`as-path-string`*
Mode	Route Map Configuration

set comm-list delete

To remove BGP communities from an inbound or outbound UPDATE message, use the set comm-list delete command in Route Map Configuration mode. A route map with this set command can be used to remove selected communities from inbound and outbound routes. When a community list is applied to a route for this purpose, each of the route's communities is submitted to the community list one at a time. Communities permitted by the list are removed from the route. Because communities are processed individually, a community list used to remove communities should not include the exact-match option on statements with multiple communities. Such statements can never match an individual community.

When a route map statement includes both set community and set comm-list delete terms, the set comm-list delete term is processed first, and then the set community term (meaning that, communities are first removed, and then communities are added).

Format	`set comm-list` *`community-list-name`* `delete`
Mode	Route Map Configuration

Parameter	Description
`community-list-name`	A standard community list name.

no set comm-list

To delete the set command from a route map, use the no form of this command.

Format	`no set comm-list`
Mode	Route Map Configuration

set community

To modify the communities attribute of matching routes, use the set community command in Route Map Configuration mode. The set community command can be used to assign communities to routes originated through BGP's network and redistribute commands, and to set communities on routes received from a specific neighbor or advertised to a specific neighbor. It can also be used to remove all communities from a route.

To remove a subset of the communities on a route, use the command set comm-list delete on page 542.

Format	`set community {`*`community-number`* `[additive] | none}`
Mode	Route Map Configuration

Parameter	Description
community-number	One to sixteen community numbers, either as a 32-bit integers or in AA:NN format. Communities are separated by spaces. The well-known communities no advertise and no-export are also accepted.
additive	(Optional) Communities are added to those already attached to the route.
none	(Optional) Removes all communities from matching routes.

no set community

To remove a set term from a route map, use the no form of this command.

Format	`no set community`
Mode	Route Map Configuration

set interface

If network administrator does not want to revert to normal forwarding but instead want to drop a packet that does not match the specified criteria, a set statement needs to be configured to route the packets to interface null 0 as the last entry in the route-map. set interface null0 needs to be configured in a separate statement. It should not be added along with any other statement having other match/set terms.

A route-map statement that is used for PBR is configured as permit or deny. If the statement is marked as deny, traditional destination-based routing is performed on the packet meeting the match criteria. If the statement is marked as permit, and if the packet meets all the match criteria, then set commands in

the route-map statement are applied. If no match is found in the route-map, the packet is not dropped, instead the packet is forwarded using the routing decision taken by performing destination-based routing.

Format	`set interface null0`
Mode	Route Map Configuration

set ip next-hop

Use this command to specify the adjacent next-hop router in the path toward the destination to which the packets should be forwarded. If more than one IP address is specified, the first IP address associated with a currently up-connected interface is used to route the packets.

This command affects all incoming packet types and is always used if configured. If configured next-hop is not present in the routing table, an ARP request is sent from the router.

In a route-map statement, 'set ip next-hop' and 'set ip default next-hop' terms are mutually exclusive. However, a 'set ip default next-hop' can be configured in a separate route-map statement.

Format	`set ip next-hop` *`ip-address [...ip-address]`*
Mode	Route Map Configuration

Parameter	Description
`ip-address`	The IP address of the next hop to which packets are output. It must be the address of an adjacent router. A maximum of 16 next-hop IP addresses can be specified in this 'set' clause.

no set ip next-hop

Use this command to remove a set command from a route map.

Format	`no set ip next-hop` *`ip-address [...ip-address]`*
Mode	Route Map Configuration

set ip default next-hop

Use this command to set a list of default next-hop IP addresses. If more than one IP address is specified, the first next hop specified that appears to be adjacent to the router is used. The optional specified IP addresses are tried in turn.

A packet is routed to the next hop specified by this command only if there is no explicit route for the packet's destination address in the routing table. A default route in the routing table is not considered an explicit route for an unknown destination address.

In a route-map statement, 'set ip next-hop' and 'set ip default next-hop' terms are mutually exclusive.However, a 'set ip next-hop' can be configured in a separate route-map statement

Format	`set ip default next-hop` *`ip-address [...ip-address]`*
Mode	Route Map Configuration

Parameter	Description
`ip-address`	The IP address of the next hop to which packets are output. It must be the address of an adjacent router. A maximum of 16 next-hop IP addresses can be specified in this 'set' clause.

no set ip default next-hop

Use this command to remove a set command from a route map.

Format	`no set ip default next-hop` *`ip-address [...ip-address]`*
Mode	Route Map Configuration

set ip precedence

Use this command to set the three IP precedence bits in the IP packet header. With three bits, you have eight possible values for the IP precedence; values 0 through 7 are defined. This command is used when implementing *QoS (Quality of Service)* and can be used by other QoS services, such as weighted fair queuing (WFQ) and weighted random early detection (WRED).

Format	`set ip precedence` *`0-7`*
Mode	Route Map Configuration

Parameter	Description
0	Sets the routine precedence
1	Sets the priority precedence
2	Sets the immediate precedence
3	Sets the Flash precedence
4	Sets the Flash override precedence
5	Sets the critical precedence
6	Sets the internetwork control precedence
7	Sets the network control precedence

no set ip precedence

Use this command to reset the three IP precedence bits in the IP packet header to the default.

Format	`no set ip precedence`
Mode	Route Map Configuration

set ipv6 next-hop (BGP)

To set the IPv6 next hop of a route, use the set ipv6 next-hop command in Route Map Configuration mode. When used in a route map applied to UPDATE messages received from a neighbor, the command sets the next hop address for matching IPv6 routes received from the neighbor.

When used in a route map applied to UPDATE messages sent to a neighbor, the command sets the next hop address for matching IPv6 routes sent to the neighbor. If the address is a link local address, the address is assumed to be on the interface where the UPDATE is sent or received. If the command specifies a global IPv6 address, the address is not required to be on a local subnet.

Format	`set ipv6 next-hop` *`ipv6-address`*
Mode	Route Map Configuration

Parameter	Description
`ipv6-address`	The IPv6 address set as the Network Address of Next Hop field in the MP_NLRI attribute of an UPDATE message.

no set ipv6 next-hop (BGP)

To remove a set command from a route map, use the no form of this command.

Format	`no set ipv6 next-hop`
Mode	Route Map Configuration

set local-preference

To set the local preference of specific BGP routes, use the `set local-preference` command in Route Map Configuration mode. The local preference is the first attribute used to compare BGP routes. Setting the local preference can influence which route BGP selects as the best route. When used in conjunction with a `match-as-path` or `match ip address` command, this command can be used to prefer routes that transit certain ASs or to make the local router a more preferred exit point to certain destinations.

Format	`set local-preference` *`value`*
Mode	Route Map Configuration

Parameter	Description
`value`	A local preference value, from 0 to 4,294,967,295 (any 32-bit integer).

no set local-preference

To remove a set command from a route map, use the no form of this command.

Format	`no set local-preference` *value*
Mode	Route Map Configuration

set metric (BGP)

To set the metric of a route, use the set metric command in Route Map Configuration mode. This command sets the Multi Exit Discriminator (MED) when used in a BGP context. When there are multiple peering points between two autonomous systems (AS), setting the MED on routes advertised by one router can influence the other AS to send traffic through a specific peer.

Format	`set metric` *value*
Mode	Route Map Configuration

Parameter	Description
value	A metric value, from 0 to 4,294,967,295 (any 32-bit integer).

no set metric (BGP)

To remove a set command from a route map, use the no form of this command.

Format	`no set metric` *value*
Mode	Route Map Configuration

show ip policy

This command lists the route map associated with each interface.

Format	`show ip policy`
Mode	Privileged EXEC

Column	Meaning
Interface	The interface.
Route-map	The route map

show ip prefix-list

This command displays configuration and status for a prefix list.

Format	`show ip prefix-list [detail | summary]` *prefix-list-name* `[`*network/length*`] [`**`seq`** *sequence-number*`] [`**`longer`**`] [`**`first-match`**`]`
Mode	Privileged EXEC

Parameter	Description
detail | summary	(Optional) Displays detailed or summarized information about all prefix lists.
prefix-list-name	(Optional) The name of a specific prefix list.
network/length	(Optional) The network number and length (in bits) of the network mask.
seq	(Optional) Applies the sequence number to the prefix list entry.
sequence-number	(Optional) The sequence number of the prefix list entry.
longer	(Optional) Displays all entries of a prefix list that are more specific than the given network/length.
first-match	(Optional) Displays the entry of a prefix list that matches the given network/length.

Acceptable forms of this command are as follows:

```
show ip prefix-list prefix-list-name network/length first-match
show ip prefix-list prefix-list-name network/length longer
show ip prefix-list prefix-list-name network/length
show ip prefix-list prefix-list-name seq sequence-number
show ip prefix-list prefix-list-name
show ip prefix-list summary
show ip prefix-list summary prefix-list-name
show ip prefix-list detail
show ip prefix-list detail prefix-list-name
```

The following example shows CLI display output for the command.

```
(Extreme 220) (Routing) #show ip prefix-list fred
ip prefix-list fred:
   count: 3, range entries: 3, sequences: 5 - 15, refcount: 0
   seq 5 permit 10.10.1.1/20 ge 22
   seq 10 permit 10.10.1.2/20 le 30
   seq 15 permit 10.10.1.2/20 ge 29 le 30
```

The following example shows CLI display output for the command.

```
(Extreme 220) (Routing) #show ip prefix-list summary fred
ip prefix-list fred:
   count: 3, range entries: 3, sequences: 5 - 15, refcount: 0
```

The following example shows CLI display output for the command.

```
(Extreme 220) (Routing) #show ip prefix-list detail fred
ip prefix-list fred:
   count: 3, range entries: 3, sequences: 5 - 15, refcount: 0
   seq 5 permit 10.10.1.1/20 ge 22 (hitcount: 0)
   seq 10 permit 10.10.1.2/20 le 30 (hitcount: 0)
   seq 15 permit 10.10.1.2/20 ge 29 le 30 (hitcount: 0)
```

show ipv6 prefix-list

This command displays configuration and status for a selected prefix list.

Format	`show ipv6 prefix-list [detail | summary] list-name [ipv6-prefix/prefix-length] [seq sequence-number] [longer] [first-match]`
Mode	Privileged EXEC

Parameter	Description
detail | summary	(Optional) Displays detailed or summarized information about all prefix lists.
list-name	(Optional) The name of a specific prefix list.
ipv6-prefix/ prefix-length	(Optional) The network number and length (in bits) of the network mask.
seq	(Optional) Applies the sequence number to the prefix list entry.
sequence-number	(Optional) The sequence number of the prefix list entry.
longer	(Optional) Displays all entries of a prefix list that are more specific than the given network/length.
first-match	(Optional) Displays the entry of a prefix list that matches the given network/length.

Acceptable forms of this command are as follows:

```
show ipv6 prefix-list listname ipv6-prefix/prefix-length first-match
show ipv6 prefix-list listname ipv6-prefix/prefix-length longer
show ipv6 prefix-list listname ipv6-prefix/prefix-length
show ipv6 prefix-list listname seq sequence-number
show ipv6 prefix-list listname
show ipv6 prefix-list summary
show ipv6 prefix-list summary prefix-list-name
show ipv6 prefix-list detail
show ipv6 prefix-list detail prefix-list-name
```

The command outputs the following information.

Column	Meaning
count	Number of entries in the prefix list.
range entries	Number of entries that match the input range.
ref count	Number of entries referencing the given prefix list.
seq	Sequence number of the entry in the list.
permit/deny	The action to take.
sequences	Range of sequence numbers for the entries in the list
hit count	Number of matches for the prefix entry

The following example shows CLI display output for the command.

```
(Extreme 220) #show ipv6 prefix-list apple
ipv6 prefix-list apple:
count: 6, range entries: 3, sequences: 5 - 30, refcount: 31
```

```
seq 5 deny 5F00::/8 le 128
seq 10 deny ::/0
seq 15 deny ::/1
seq 20 deny ::/2
seq 25 deny ::/3 ge 4
        seq 30 permit ::/0 le 128
(Extreme 220) #show ipv6 prefix-list summary apple
ipv6 prefix-list apple:
count: 6, range entries: 3, sequences: 5 - 30, refcount: 31
(Extreme 220) #show ipv6 prefix-list detail apple
ipv6 prefix-list apple:
count: 6, range entries: 3, sequences: 5 - 30, refcount: 31
seq 5 deny 5F00::/8 le 128 (hit count: 0, refcount: 1)
seq 10 deny ::/0 (hit count: 0, refcount: 1)
seq 15 deny ::/1 (hit count: 0, refcount: 1)
seq 20 deny ::/2 (hit count: 0, refcount: 1)
seq 25 deny ::/3 ge 4 (hit count: 0, refcount: 1)
        seq 30 permit ::/0 le 128 (hit count: 240664, refcount: 0)
```

show route-map

To display a route map, use the show route-map command in Privileged EXEC mode.

Format	`show route-map [map-name]`
Mode	Privileged EXEC

Parameter	Description
map-name	(Optional) Name of a specific route map.

The following example shows CLI display output for the command.

```
(Extreme 220) (Routing) # show route-map test
route-map test, permit, sequence 10
     Match clauses:
       ip address prefix-lists: orange
         Set clauses:
           set metric 50
```

clear ip prefix-list

To reset IP prefix-list counters, use the clear ip prefix-list command in Privileged EXEC mode. This command is used to clear prefix-list hit counters. The hit count is a value indicating the number of matches to a specific prefix list entry.

Format	`clear ip prefix-list [prefix-list-name] [network/length]]`
Mode	Privileged EXEC

Parameter	Description
prefix-list-name	(Optional) Name of the prefix list from which the hit count is to be cleared.
network/length	(Optional) Network number and length (in bits) of the network mask. If this option is specified, hit counters are only cleared for the matching statement.

The following shows an example of the command.

```
(Extreme 220) (Routing) # clear ip prefix-list orange 20.0.0.0/8
```

clear ipv6 prefix-list

Use this command to reset and clear IPv6 prefix-list hit counters. The hit count is a value indicating the number of matches to a specific prefix list entry.

Format	`clear ipv6 prefix-list [prefix-list-name] [ipv6-prefix/prefix-length]`
Mode	Privileged EXEC

Parameter	Description
list-name	(Optional) Name of the prefix list from which the hit count is to be cleared.
ipv6-prefix/prefix-length	(Optional) IPv6 prefix number and length (in bits) of the network mask. If this option is specified, hit counters are only cleared for the matching statement.

Virtual LAN Routing Commands

This section describes the commands used to view and configure VLAN routing and to view VLAN routing status information.

vlan routing

This command enables routing on a VLAN. The vlanid value has a range from 1 to 4093. The [interface ID] value has a range from 1 to 128. Typically, you will not supply the interface ID argument, and the system automatically selects the interface ID. However, if you specify an interface ID, the interface ID becomes the port number in the unit/slot/port for the VLAN routing interface. If you select an interface ID that is already in use, the CLI displays an error message and does not create the VLAN interface. For products that use text-based configuration, including the interface ID in the vlan routing command for the text configuration ensures that the unit/slot/port for the VLAN interface stays the same across a restart. Keeping the unit/slot/port the same ensures that the correct interface configuration is applied to each interface when the system restarts.

Format	`vlan routing vlanid [interface ID]`
Mode	VLAN Config

no vlan routing

This command deletes routing on a VLAN.

Format	`no vlan routing vlanid`
Mode	VLAN Config

Example 1 shows the command specifying a vlanid value. The interface ID argument is not used.

```
(Extreme 220)(Vlan)#vlan 14
(Extreme 220)(Vlan)#vlan routing 14 ?
<cr>                    Press enter to execute the command.
<1-24>                 Enter interface ID
```

Typically, you press <Enter> without supplying the Interface ID value; the system automatically selects the interface ID.

In Example 2, the command specifies interface ID 51 for VLAN 14 interface. The interface ID becomes the port number in the unit/slot/port for the VLAN routing interface. In this example, unit/slot/port is 4/51 for VLAN 14 interface.

```
(Extreme 220)(Vlan)#vlan 14 51
(Extreme 220)(Vlan)#
(Extreme 220) #show ip vlan
MAC Address used by Routing VLANs:   00:11:88:59:47:36
           Logical
VLAN ID   Interface        IP Address       Subnet Mask
-------  --------------  ---------------  ---------------
10       4/1             172.16.10.1      255.255.255.0
11       4/50            172.16.11.1      255.255.255.0
12       4/3             172.16.12.1      255.255.255.0
13       4/4             172.16.13.1      255.255.255.0
14       4/51            0.0.0.0          0.0.0.0                                    <--
u/s/p is 4/51 for VLAN 14 interface
```

In Example 3, you select an interface ID that is already in use. In this case, the CLI displays an error message and does not create the VLAN interface.

```
(Extreme 220) #show ip vlan
MAC Address used by Routing VLANs:   00:11:88:59:47:36
           Logical
VLAN ID   Interface        IP Address       Subnet Mask
-------  --------------  ---------------  ---------------
10       4/1             172.16.10.1      255.255.255.0
11       4/50            172.16.11.1      255.255.255.0
12       4/3             172.16.12.1      255.255.255.0
13       4/4             172.16.13.1      255.255.255.0
14       4/51            0.0.0.0          0.0.0.0
(Extreme 220) #config
(Extreme 220) (Config)#exit
(Extreme 220) (Config) #vlan database
(Extreme 220)(Vlan)#vlan 15
(Extreme 220)(Vlan)#vlan routing 15 1
Interface ID 1 is already assigned to another interface
```

The show running configuration command always lists the interface ID for each routing VLAN, as shown in Example 4.

```
(Extreme 220) #show running-config
!!Current Configuration:
!
!System Description "Extreme 220-Series 24GE, 2 10GbE SFP+ ports, 1 Fixed AC PSU
, 1 RPS port, L3 Switching, 1.1.1.10, Linux 3.6.5, U-Boot 2012.10-gac78d49 (Jan
09 2017 - 11:09:03)"
!System Software Version "R.7.28.4"
!System Up Time          "0 days 8 hrs 38 mins 3 secs"
!Cut-through mode is configured as disabled
!Additional Packages     FASTPATH BGP-4,FASTPATH QOS,FASTPATH Multicast,FASTPATH
```

```
IPv6,FASTPATH IPv6 Management,FASTPATH Metro,FASTPATH Routing,FASTPATH Data Center
!Current SNTP Synchronized Time: SNTP Client Mode Is Disabled
!
vlan database
exit
configure
no logging console
aaa authentication enable "enableNetList" none
line console
serial timeout 0
exit
line telnet
exit
line ssh
exit
!
router rip
exit
router ospf
exit
ipv6 router ospf
exit
exit
```

interface vlan

Use this command to enter Interface configuration mode for the specified VLAN. The vlan-id range is 1 to 4093.

Format	`interface vlan vlan-id`
Mode	Global Config

show ip vlan

This command displays the VLAN routing information for all VLANs with routing enabled.

Format	`show ip vlan`
Modes	• Privileged EXEC • User EXEC

Term	Definition
MAC Address used by Routing VLANs	The MAC Address associated with the internal bridge-router interface (IBRI). The same MAC Address is used by all VLAN routing interfaces. It will be displayed above the per-VLAN information.
VLAN ID	The identifier of the VLAN.
Logical Interface	The logical *unit/slot/port* associated with the VLAN routing interface.
IP Address	The IP address associated with this VLAN.

Term	Definition
Subnet Mask	The subnet mask that is associated with this VLAN.

DHCP and BOOTP Relay Commands

This section describes the commands used to configure BootP/DHCP Relay on the switch. A *DHCP* relay agent operates at Layer 3 and forwards DHCP requests and replies between clients and servers when they are not on the same physical subnet.

bootpdhcprelay cidoptmode

This command enables the circuit ID option mode for BootP/DHCP Relay on the system.

Default	disabled
Format	`bootpdhcprelay cidoptmode`
Mode	• Global Config • Virtual Router Config

no bootpdhcprelay cidoptmode

This command disables the circuit ID option mode for BootP/DHCP Relay on the system.

Format	`no bootpdhcprelay cidoptmode`
Mode	• Global Config • Virtual Router Config

bootpdhcprelay maxhopcount

This command configures the maximum allowable relay agent hops for BootP/DHCP Relay on the system. The hops parameter has a range of 1 to 16.

Default	4
Format	`bootpdhcprelay maxhopcount` *1-16*
Mode	• Global Config • Virtual Router Config

no bootpdhcprelay maxhopcount

This command configures the default maximum allowable relay agent hops for BootP/DHCP Relay on the system.

Format	`no bootpdhcprelay maxhopcount`
Mode	• Global Config • Virtual Router Config

bootpdhcprelay minwaittime

This command configures the minimum wait time in seconds for BootP/DHCP Relay on the system. When the BOOTP relay agent receives a BOOTREQUEST message, it MAY use the seconds-since-client-began-booting field of the request as a factor in deciding whether to relay the request or not. The parameter has a range of 0 to 100 seconds.

Default	0
Format	`bootpdhcprelay minwaittime` *`0-100`*
Mode	• Global Config • Virtual Router Config

no bootpdhcprelay minwaittime

This command configures the default minimum wait time in seconds for BootP/DHCP Relay on the system.

Format	`no bootpdhcprelay minwaittime`
Mode	• Global Config • Virtual Router Config

bootpdhcprelay serverip

This command configures the server IP address of the BootP/DHCP Relay on the system. The ipaddr parameter is the IP address of the server.

Default	0.0.0.0
Format	`bootpdhcprelay serverip` *`ipaddr`*
Mode	Global Config

no bootpdhcprelay serverip

This command returns the server IP address of the BootP/DHCP Relay on the system to the default value of 0.0.0.0.

Format	`no bootpdhcprelay serverip`
Mode	Global Config

bootpdhcprelay enable

Use this command to enable the relay of *DHCP* packets.

Default	disabled
Format	`bootpdhcprelay enable`
Mode	Global Config

no bootpdhcprelay enable

Use this command to disable the relay of *DHCP* packets.

Default	disabled
Format	`no bootpdhcprelay enable`
Mode	Global Config

show bootpdhcprelay

This command displays the BootP/DHCP Relay information.

Format	`show bootpdhcprelay`
Modes	• Privileged EXEC • User EXEC

Term	Definition
Maximum Hop Count	The maximum allowable relay agent hops.
Minimum Wait Time (Seconds)	The minimum wait time.
Admin Mode	Whether relaying of requests is enabled or disabled.
Circuit Id Option Mode	The DHCP circuit Id option which may be enabled or disabled.

show ip bootpdhcprelay

This command displays BootP/DHCP Relay information.

Format	`show ip bootpdhcprelay`
Modes	• Privileged EXEC • User EXEC

Parameter	Definition
Maximum Hop Count	The maximum allowable relay agent hops.
Minimum Wait Time (Seconds)	The minimum wait time.
Admin Mode	Whether relaying of requests is enabled or disabled.
Circuit Id Option Mode	The DHCP circuit Id option which may be enabled or disabled.

The following shows an example of the command.

```
(Extreme 220) (Routing) #show ip bootpdhcprelay
Maximum Hop Count.............................. 4
Minimum Wait Time(Seconds)..................... 0
Admin Mode..................................... Disable
Circuit Id Option Mode......................... Enable
```

IP Helper Commands

This section describes the commands to configure and monitor the IP Helper agent. IP Helper relays *DHCP* and other broadcast UDP packets from a local client to one or more servers which are not on the same network at the client.

The IP Helper feature provides a mechanism that allows a router to forward certain configured UDP broadcast packets to a particular IP address. This allows various applications to reach servers on nonlocal subnets, even if the application was designed to assume a server is always on a local subnet and uses broadcast packets (with either the limited broadcast address 255.255.255.255, or a network directed broadcast address) to reach the server.

The network administrator can configure relay entries both globally and on routing interfaces. Each relay entry maps an ingress interface and destination UDP port number to a single IPv4 address (the helper address). The network administrator may configure multiple relay entries for the same interface and UDP port, in which case the relay agent relays matching packets to each server address. Interface configuration takes priority over global configuration. That is, if a packet's destination UDP port matches any entry on the ingress interface, the packet is handled according to the interface configuration. If the packet does not match any entry on the ingress interface, the packet is handled according to the global IP helper configuration.

The network administrator can configure discard relay entries, which direct the system to discard matching packets. Discard entries are used to discard packets received on a specific interface when those packets would otherwise be relayed according to a global relay entry. Discard relay entries may be configured on interfaces, but are not configured globally.

In addition to configuring the server addresses, the network administrator also configures which UDP ports are forwarded. Certain UDP port numbers can be specified by name in the UI as a convenience, but the network administrator can configure a relay entry with any UDP port number. The network administrator may configure relay entries that do not specify a destination UDP port. The relay agent relays assumes these entries match packets with the UDP destination ports listed in Table 12. This is the list of default ports.

Table 12: Default Ports - UDP Port Numbers Implied by Wildcard

Protocol	UDP Port Number
IEN-116 Name Service	42
DNS	53
NetBIOS Name Server	137
NetBIOS Datagram Server	138
TACACS Server	49
Time Service	37
DHCP	67
Trivial File Transfer Protocol (TFTP)	69

The system limits the number of relay entries to four times the maximum number of routing interfaces. The network administrator can allocate the relay entries as he likes. There is no limit to the number of relay entries on an individual interface, and no limit to the number of servers for a given {interface, UDP port} pair.

The relay agent relays DHCP packets in both directions. It relays broadcast packets from the client to one or more DHCP servers, and relays to the client packets that the DHCP server unicasts back to the relay agent. For other protocols, the relay agent only relays broadcast packets from the client to the server. Packets from the server back to the client are assumed to be unicast directly to the client. Because there is no relay in the return direction for protocols other than DHCP, the relay agent retains the source IP address from the original client packet. The relay agent uses a local IP address as the source IP address of relayed DHCP client packets.

When a switch receives a broadcast UDP packet on a routing interface, the relay agent checks if the interface is configured to relay the destination UDP port. If so, the relay agent unicasts the packet to the configured server IP addresses. Otherwise, the relay agent checks if there is a global configuration for the destination UDP port. If so, the relay agent unicasts the packet to the configured server IP addresses. Otherwise the packet is not relayed. Note that if the packet matches a discard relay entry on the ingress interface, then the packet is not forwarded, regardless of the global configuration.

The relay agent only relays packets that meet the following conditions:

- The destination MAC address must be the all-ones broadcast address (FF:FF:FF:FF:FF:FF)
- The destination IP address must be the limited broadcast address (255.255.255.255) or a directed broadcast address for the receive interface.
- The IP time-to-live (TTL) must be greater than 1.
- The protocol field in the IP header must be UDP (17).
- The destination UDP port must match a configured relay entry.

clear ip helper statistics

Use this command to reset to zero the statistics displayed in the `show ip helper statistics` command.

Format	`clear ip helper statistics`
Mode	Privileged EXEC

The following shows an example of the command.

```
(Extreme 220) #clear ip helper statistics
```

ip helper-address (Global Config)

Use this command to configure the relay of certain UDP broadcast packets received on any interface. This command can be invoked multiple times, either to specify multiple server addresses for a given UDP port number or to specify multiple UDP port numbers handled by a specific server.

Default	No helper addresses are configured.
Format	`ip helper-address server-address [dest-udp-port | dhcp | domain | isakmp | mobile-ip | nameserver | netbios-dgm | netbios-ns | ntp | pim-auto-rp | rip | tacacs | tftp | time]`
Mode	• Global Config • Virtual Router Config

Parameter	Description
server-address	The IPv4 unicast or directed broadcast address to which relayed UDP broadcast packets are sent. The server address cannot be an IP address configured on any interface of the local router.
dest-udp-port	A destination UDP port number from 0 to 65535.
port-name	The destination UDP port may be optionally specified by its name. Whether a port is specified by its number or its name has no effect on behavior. The names recognized are as follows: • dhcp (port 67) • domain (port 53) • isakmp (port 500) • mobile-ip (port 434) • nameserver (port 42) • netbios-dgm (port 138) • netbios-ns (port 137) • ntp (port 123) • pim-auto-rp (port 496) • rip (port 520) • tacacs (port 49) • tftp (port 69) • time (port 37) Other ports must be specified by number.

To relay *DHCP* packets received on any interface to two DHCP servers, 10.1.1.1 and 10.1.2.1, use the following commands:

```
(Extreme 220) #config
(Extreme 220) (Config) #ip helper-address 10.1.1.1 dhcp
(Extreme 220) (Config) #ip helper-address 10.1.2.1 dhcp
```

To relay UDP packets received on any interface for all default ports to the server at 20.1.1.1, use the following commands:

```
(Extreme 220) #config
(Extreme 220) (Config) #ip helper-address 20.1.1.1
```

no ip helper-address (Global Config)

Use the no form of the command to delete an IP helper entry. The command no ip helper-address with no arguments clears all global IP helper addresses.

Format	`no ip helper-address [server-address [dest-udp-port | dhcp | domain | isakmp | mobile-ip | nameserver | netbios-dgm | netbios-ns | ntp | pim-auto-rp | rip | tacacs | tftp | time]`
Mode	Global Config

ip helper-address (Interface Config)

Use this command to configure the relay of certain UDP broadcast packets received on a specific interface or range of interfaces. This command can be invoked multiple times on a routing interface, either to specify multiple server addresses for a given port number or to specify multiple port numbers handled by a specific server.

Default	No helper addresses are configured.
Format	`ip helper-address {server-address | discard} [dest-udp-port | dhcp | domain | isakmp | mobile ip | nameserver | netbios-dgm | netbios-ns | ntp | pim-auto-rp | rip | tacacs | tftp | time]`
Mode	Interface Config

Parameter	Description
server-address	The IPv4 unicast or directed broadcast address to which relayed UDP broadcast packets are sent. The server address cannot be in a subnet on the interface where the relay entry is configured, and cannot be an IP address configured on any interface of the local router.
discard	Matching packets should be discarded rather than relayed, even if a global ip helper-address configuration matches the packet.

Parameter	Description
dest-udp-port	A destination UDP port number from 0 to 65535.
port-name	The destination UDP port may be optionally specified by its name. Whether a port is specified by its number or its name has no effect on behavior. The names recognized are as follows: • dhcp (port 67) • domain (port 53) • isakmp (port 500) • mobile-ip (port 434) • nameserver (port 42) • netbios-dgm (port 138) • netbios-ns (port 137) • ntp (port 123) • pim-auto-rp (port 496) • rip (port 520) • tacacs (port 49) • tftp (port 69) • time (port 37) Other ports must be specified by number.

To relay *DHCP* packets received on interface 1/0/2 to two DHCP servers, 192.168.10.1 and 192.168.20.1, use the following commands:

```
(Extreme 220) #config
(Extreme 220) (Config) #interface 1/0/2
(Extreme 220)(interface 1/0/2)#ip helper-address 192.168.10.1 dhcp
(Extreme 220)(interface 1/0/2)#ip helper-address 192.168.20.1 dhcp
```

To relay both DHCP and DNS packets to 192.168.30.1, use the following commands:

```
(Extreme 220) #config
(Extreme 220) (Config) #interface 1/0/2
(Extreme 220)(interface 1/0/2)#ip helper-address 192.168.30.1 dhcp
(Extreme 220)(interface 1/0/2)#ip helper-address 192.168.30.1 dns
```

This command takes precedence over an ip helper-address command given in global configuration mode. With the following configuration, the relay agent relays DHCP packets received on any interface other than 1/0/2 and 1/0/17 to 192.168.40.1, relays DHCP and DNS packets received on 1/0/2 to 192.168.40.2, relays *SNMP (Simple Network Management Protocol)* traps (port 162) received on interface 1/0/17 to 192.168.23.1, and drops DHCP packets received on 1/0/17:

```
(Extreme 220) #config
(Extreme 220) (Config) #ip helper-address 192.168.40.1 dhcp
(Extreme 220) (Config) #interface 1/0/2
(Extreme 220)(interface 1/0/2)#ip helper-address 192.168.40.2 dhcp
(Extreme 220)(interface 1/0/2)#ip helper-address 192.168.40.2 domain
(Extreme 220)(interface 1/0/2)#exit
(Extreme 220) (Config) #interface 1/0/17
(Extreme 220)(interface 1/0/17)#ip helper-address 192.168.23.1 162
(Extreme 220)(interface 1/0/17)#ip helper-address discard dhcp
```

no ip helper-address (Interface Config)

Use this command to delete a relay entry on an interface. The `no` command with no arguments clears all helper addresses on the interface.

Format	`no ip helper-address [server-address | discard ][dest-udp-port | dhcp | domain | isakmp | mobile ip | nameserver | netbios-dgm | netbios-ns | ntp | pim-auto-rp | rip | tacacs | tftp | time]`
Mode	Interface Config

ip helper enable

Use this command to enable relay of UDP packets. This command can be used to temporarily disable IP helper without deleting all IP helper addresses. This command replaces the `bootpdhcprelay enable` command, but affects not only relay of *DHCP* packets, but also relay of any other protocols for which an IP helper address has been configured.

Default	disabled
Format	`ip helper enable`
Mode	• Global Config • Virtual Router Config

The following shows an example of the command.

```
(Extreme 220) (Config)#ip helper enable
```

no ip helper enable

Use the no form of this command to disable relay of all UDP packets.

Format	`no ip helper enable`
Mode	Global Config

show ip helper-address

Use this command to display the IP helper address configuration. The argument unit/slot/port corresponds to a physical routing interface or VLAN routing interface. The keyword **`vlan`** is used to specify the VLAN ID of the routing VLAN directly instead of a unit/slot/port format.

Format	`show ip helper-address` *`unit/slot/port|vlan 1-4093}`*`]`
Mode	Privileged EXEC

Parameter	Description
interface	The relay configuration is applied to packets that arrive on this interface. This field is set to **any** for global IP helper entries.
UDP Port	The relay configuration is applied to packets whose destination UDP port is this port. Entries whose UDP port is identified as any are applied to packets with the destination UDP ports listed in Table 4.
Discard	If Yes, packets arriving on the given interface with the given destination UDP port are discarded rather than relayed. Discard entries are used to override global IP helper address entries which otherwise might apply to a packet.
Hit Count	The number of times the IP helper entry has been used to relay or discard a packet.
Server Address	The IPv4 address of the server to which packets are relayed.

The following example shows CLI display output for the command.

```
(Extreme 220) #show ip helper-address
IP helper is enabled
    Interface   UDP Port     Discard   Hit Count   Server Address
---------------  -----------  --------  ----------  ---------------
          1/0/1       dhcp        No         10         10.100.1.254
                                                     10.100.2.254
          1/0/17      any        Yes          2
          any         dhcp        No          0         10.200.1.254
```

show ip helper statistics

Use this command to display the number of *DHCP* and other UDP packets processed and relayed by the UDP relay agent.

Format	`show ip helper statistics`
Mode	Privileged EXEC

Parameter	Description
DHCP client messages received	The number of valid messages received from a DHCP client. The count is only incremented if IP helper is enabled globally, the ingress routing interface is up, and the packet passes a number of validity checks, such as having a TTL>1 and having valid source and destination IP addresses.
DHCP client messages relayed	The number of DHCP client messages relayed to a server. If a message is relayed to multiple servers, the count is incremented once for each server.
DHCP server messages received	The number of DHCP responses received from the DHCP server. This count only includes messages that the DHCP server unicasts to the relay agent for relay to the client.
DHCP server messages relayed	The number of DHCP server messages relayed to a client.

Parameter	Description
UDP clients messages received	The number of valid UDP packets received. This count includes DHCP messages and all other protocols relayed. Conditions are similar to those for the first statistic in this table.
UDP clients messages relayed	The number of UDP packets relayed. This count includes DHCP messages relayed as well as all other protocols. The count is incremented for each server to which a packet is sent.
DHCP message hop count exceeded max	The number of DHCP client messages received whose hop count is larger than the maximum allowed. The maximum hop count is a configurable value listed in show bootpdhcprelay. A log message is written for each such failure. The DHCP relay agent does not relay these packets.
DHCP message with secs field below min	The number of DHCP client messages received whose secs field is less than the minimum value. The minimum secs value is a configurable value and is displayed in show bootpdhcprelay. A log message is written for each such failure. The DHCP relay agent does not relay these packets.
DHCP message with giaddr set to local address	The number of DHCP client messages received whose gateway address, giaddr, is already set to an IP address configured on one of the relay agent's own IP addresses. In this case, another device is attempting to spoof the relay agent's address. The relay agent does not relay such packets. A log message gives details for each occurrence.
Packets with expired TTL	The number of packets received with TTL of 0 or 1 that might otherwise have been relayed.
Packets that matched a discard entry	The number of packets ignored by the relay agent because they match a discard relay entry.

The following example shows CLI display output for the command.

```
(Extreme 220) #show ip helper statistics
DHCP client messages received..................... 8
DHCP client messages relayed...................... 2
DHCP server messages received..................... 2
DHCP server messages relayed...................... 2
UDP client messages received...................... 8
UDP client messages relayed....................... 2
DHCP message hop count exceeded max............... 0
DHCP message with secs field below min......... 0
DHCP message with giaddr set to local address.. 0
Packets with expired TTL.......................... 0
Packets that matched a discard entry........... 0
```

Routing Information Protocol Commands

This section describes the commands used to view and configure *RIP*, which is a distance-vector routing protocol for routing traffic within a small network.

router rip

Use this command to enter Router *RIP* mode.

Format	`router rip`
Mode	Global Config

enable (RIP)

This command resets the default administrative mode of *RIP* in the router (active).

Default	enabled
Format	`enable`
Mode	Router RIP Config

no enable (RIP)

This command sets the administrative mode of *RIP* in the router to inactive.

Format	`no enable`
Mode	Router RIP Config

ip rip

This command enables *RIP* on a router interface or range of interfaces.

Default	disabled
Format	`ip rip`
Mode	Interface Config

no ip rip

This command disables *RIP* on a router interface.

Format	`no ip rip`
Mode	Interface Config

auto-summary

This command enables the *RIP* auto-summarization mode.

Default	disabled
Format	`auto-summary`
Mode	Router RIP Config

no auto-summary

This command disables the *RIP* auto-summarization mode.

Format	`no auto-summary`
Mode	Router RIP Config

default-information originate (RIP)

This command is used to control the advertisement of default routes.

Format	`default-information originate`
Mode	Router *RIP* Config

no default-information originate (RIP)

This command is used to control the advertisement of default routes.

Format	`no default-information originate`
Mode	Router *RIP* Config

default-metric (RIP)

This command is used to set a default for the metric of distributed routes.

Format	`default-metric` *0–15*
Mode	Router *RIP* Config

no default-metric (RIP)

This command is used to reset the default metric of distributed routes to its default value.

Format	`no default-metric`
Mode	Router *RIP* Config

distance rip

This command sets the route preference value of *RIP* in the router. Lower route preference values are preferred when determining the best route. A route with a preference of 255 cannot be used to forward traffic.

Default	15
Format	`distance rip 1-255`
Mode	Router RIP Config

no distance rip

This command sets the default route preference value of *RIP* in the router.

Format	`no distance rip`
Mode	Router RIP Config

distribute-list out (RIP)

This command is used to specify the access list to filter routes received from the source protocol.

Default	0
Format	`distribute-list 1-199 out {ospf | bgp | static | connected}`
Mode	Router *RIP* Config

no distribute-list out

This command is used to specify the access list to filter routes received from the source protocol.

Format	`no distribute-list 1-199 out {ospf | bgp | static | connected}`
Mode	Router *RIP* Config

ip rip authentication

This command sets the *RIP* Version 2 Authentication Type and Key for the specified interface or range of interfaces. The value of type is either none, simple, or encrypt. The value for authentication key [key] must be 16 bytes or less. The [key] is composed of standard displayable, noncontrol keystrokes from a Standard 101/102-key keyboard. If the value of type is encrypt, a keyid in the range of 0 and 255 must be specified. Unauthenticated interfaces do not need an authentication key or authentication key ID.

Default	none
Format	`ip rip authentication {none | {simple` *`key`*`} | {encrypt` *`key keyid`*`}}`
Mode	Interface Config

no ip rip authentication

This command sets the default *RIP* Version 2 Authentication Type for an interface.

Format	`no ip rip authentication`
Mode	Interface Config

ip rip receive version

This command configures an interface or range of interfaces to allow *RIP* control packets of the specified version(s) to be received.

The value for mode is one of: rip1 to receive only RIP version 1 formatted packets, rip2 for RIP version 2, both to receive packets from either format, or none to not allow any RIP control packets to be received.

Default	both
Format	`ip rip receive version {rip1 | rip2 | both | none}`
Mode	Interface Config

no ip rip receive version

This command configures the interface to allow *RIP* control packets of the default version(s) to be received.

Format	`no ip rip receive version`
Mode	Interface Config

ip rip send version

This command configures an interface or range of interfaces to allow *RIP* control packets of the specified version to be sent. The value for mode is one of: rip1 to broadcast RIP version 1 formatted packets, rip1c (RIP version 1 compatibility mode) which sends RIP version 2 formatted packets via broadcast, rip2 for sending RIP version 2 using multicast, or none to not allow any RIP control packets to be sent.

Default	rip2
Format	`ip rip send version {rip1 | rip1c | rip2 | none}`
Mode	Interface Config

no ip rip send version

This command configures the interface to allow *RIP* control packets of the default version to be sent.

Format	`no ip rip send version`
Mode	Interface Config

hostroutesaccept

This command enables the *RIP* hostroutesaccept mode.

Default	enabled
Format	`hostroutesaccept`
Mode	Router RIP Config

no hostroutesaccept

This command disables the *RIP* hostroutesaccept mode.

Format	`no hostroutesaccept`
Mode	Router RIP Config

split-horizon

This command sets the *RIP* split horizon mode. Split horizon is a technique for avoiding problems caused by including routes in updates sent to the router from which the route was originally learned. The options are: None - no special processing for this case. Simple - a route will not be included in updates sent to the router from which it was learned. Poisoned reverse - a route will be included in updates sent to the router from which it was learned, but the metric will be set to infinity.

Default	simple
Format	`split-horizon {none | simple | poison}`
Mode	Router RIP Config

no split-horizon

This command sets the default *RIP* split horizon mode.

Format	`no split-horizon`
Mode	Router RIP Config

redistribute (RIP)

This command configures *RIP* protocol to redistribute routes from the specified source protocol/routers. There are five possible match options. When you submit the command redistribute ospf match match-type the match-type or types specified are added to any match types presently being redistributed. Internal routes are redistributed by default.

Default	• metric—not-configured • match—internal
Format for *OSPF* as source protocol	redistribute ospf [metric *0–15*] [match *[internal] [external 1] [external 2] [nssa-external 1] [nssa-external-2]*]
Format for other source protocol	redistribute {bgp | static | connected} [metric *0–15*]
Mode	Router RIP Config

no redistribute

This command de-configures *RIP* protocol to redistribute routes from the specified source protocol/ routers.

Format	`no redistribute {ospf | bgp | static | connected} [metric] [match` *`[internal] [external 1] [external 2] [nssa-external 1] [nssa-external-2]`*`]`
Mode	Router RIP Config

show ip rip

This command displays information relevant to the *RIP* router.

Format	`show ip rip`
Modes	• Privileged EXEC • User EXEC

Term	Definition
RIP Admin Mode	Enable or disable.
Split Horizon Mode	None, simple or poison reverse.
Auto Summary Mode	Enable or disable. If enabled, groups of adjacent routes are summarized into single entries, in order to reduce the total number of entries The default is enable.
Host Routes Accept Mode	Enable or disable. If enabled the router accepts host routes. The default is enable.

Term	Definition
Global Route Changes	The number of route changes made to the IP Route Database by RIP. This does not include the refresh of a route's age.
Global queries	The number of responses sent to RIP queries from other systems.
Default Metric	The default metric of redistributed routes if one has already been set, or blank if not configured earlier. The valid values are 1 to 15.
Default Route Advertise	The default route.

show ip rip interface brief

This command displays general information for each *RIP* interface. For this command to display successful results routing must be enabled per interface (that is, ip rip).

Format	`show ip rip interface brief`
Modes	• Privileged EXEC • User EXEC

Term	Definition
Interface	*unit/slot/port*
IP Address	The IP source address used by the specified RIP interface.
Send Version	The RIP version(s) used when sending updates on the specified interface. The types are none, RIP-1, RIP-1c, RIP-2
Receive Version	The RIP version(s) allowed when receiving updates from the specified interface. The types are none, RIP-1, RIP-2, Both
RIP Mode	The administrative mode of router RIP operation (enabled or disabled).
Link State	The mode of the interface (up or down).

show ip rip interface

This command displays information related to a particular *RIP* interface. The argument unit/slot/port corresponds to a physical routing interface or VLAN routing interface. The keyword **`vlan`** is used to specify the VLAN ID of the routing VLAN directly instead of a unit/slot/port format.

Format	`show ip rip interface {`*`unit/slot/port`*`|`*`vlan 1-4093`*`}`
Modes	• Privileged EXEC • User EXEC

Term	Definition
Interface	*unit/slot/port* This is a configured value.
IP Address	The IP source address used by the specified RIP interface. This is a configured value.
Send Version	The RIP version(s) used when sending updates on the specified interface. The types are none, RIP-1, RIP-1c, RIP-2. This is a configured value.
Receive Version	The RIP version(s) allowed when receiving updates from the specified interface. The types are none, RIP-1, RIP-2, Both. This is a configured value.
RIP Admin Mode	RIP administrative mode of router RIP operation; enable activates, disable de-activates it. This is a configured value.
Link State	Whether the RIP interface is up or down. This is a configured value.
Authentication Type	The RIP Authentication Type for the specified interface. The types are none, simple, and encrypt. This is a configured value.

The following information will be invalid if the link state is down.

Term	Definition
Bad Packets Received	The number of RIP response packets received by the RIP process which were subsequently discarded for any reason.
Bad Routes Received	The number of routes contained in valid RIP packets that were ignored for any reason.
Updates Sent	The number of triggered RIP updates actually sent on this interface.

7 IPv6 Management Commands

This chapter describes the IPv6 commands available in the 200 Series CLI.

Caution

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

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

IPv6 Management Commands

IPv6 Management commands allow a device to be managed via an IPv6 address in a switch or IPv4 routing (that is, independent from the IPv6 Routing package). For Routing/IPv6 builds of 200 Series dual IPv4/IPv6 operation over the service port is enabled. 200 Series 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 (Simple Network Management Protocol)* traps and queries via the service/network port.
- The user can manage a device via the network port (in addition to a Routing Interface or the Service port).

serviceport ipv6 enable

Use this command to enable IPv6 operation on the service port. By default, IPv6 operation is enabled on the service port.

Default	Enabled
Format	`serviceport ipv6 enable`
Mode	Privileged EXEC

no serviceport ipv6 enable

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

Format	`no serviceport ipv6 enable`
Mode	Privileged EXEC

network ipv6 enable

Use this command to enable IPv6 operation on the network port. By default, IPv6 operation is enabled on the network port.

Default	Enabled
Format	`network ipv6 enable`
Mode	Privileged EXEC

no network ipv6 enable

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

Format	`no network ipv6 enable`
Mode	Privileged EXEC

serviceport ipv6 address

Use this command to manually configure IPv6 global address, enable/disable stateless global address autoconfiguration and to enable/disable dhcpv6 client protocol information on the service port.

Note
Multiple IPv6 prefixes can be configured on the service port.

Format	`serviceport ipv6 address {`*`address/prefix-length`* `[eui64]| autoconfig|dhcp}`
Mode	Privileged EXEC

Parameter	Description
`address`	IPv6 prefix in IPv6 global address format.
`prefix-length`	IPv6 prefix length value.
`eui64`	Formulate IPv6 address in eui64 address format.
`autoconfig`	Configure stateless global address autoconfiguration capability.
`dhcp`	Configure dhcpv6 client protocol.

no serviceport ipv6 address

Use the command no serviceport ipv6 address to remove all configured IPv6 prefixes on the service port interface.

Use the command with the address option to remove the manually configured IPv6 global address on the network port interface.

Use the command with the autoconfig option to disable the stateless global address autoconfiguration on the service port.

Use the command with the dhcp option to disable the dhcpv6 client protocol on the service port.

Format	`no serviceport ipv6 address {`*`address/prefix-length`* `[eui64] | autoconfig | dhcp}`
Mode	Privileged EXEC

serviceport ipv6 gateway

Use this command to configure IPv6 gateway (that is, Default routers) information for the service port.

Note

Only a single IPv6 gateway address can be configured for the service port. There may be a combination of IPv6 prefixes and gateways that are explicitly configured and those that are set through auto-address configuration with a connected IPv6 router on their service port interface.

Format	`serviceport ipv6 gateway` *`gateway-address`*
Mode	Privileged EXEC

Parameter	Description
`gateway-address`	Gateway address in IPv6 global or link-local address format.

no serviceport ipv6 gateway

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

Format	`no serviceport ipv6 gateway`
Mode	Privileged EXEC

serviceport ipv6 neighbor

Use this command to manually add IPv6 neighbors to the IPv6 neighbor table for the service port. If an IPv6 neighbor already exists in the neighbor table, the entry is automatically converted to a static entry. Static entries are not modified by the neighbor discovery process. They are, however, treated the same for IPv6 forwarding. Static IPv6 neighbor entries are applied to the kernel stack and to the hardware when the corresponding interface is operationally active.

Format	`serviceport ipv6 neighbor` *`ipv6-address macaddr`*
Mode	Privileged EXEC

Parameter	Description
`ipv6-address`	The IPv6 address of the neighbor or interface.
`macaddr`	The link-layer address.

no serviceport ipv6 neighbor

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

Format	`no serviceport ipv6 neighbor` *`ipv6-address macaddr`*
Mode	Privileged EXEC

network ipv6 address

Use the options of this command to manually configure IPv6 global address, enable/disable stateless global address autoconfiguration and to enable/disable dhcpv6 client protocol information for the network port. Multiple IPv6 addresses can be configured on the network port.

Format	`network ipv6 address {`*`address/prefix-length`* `[eui64] | autoconfig | dhcp}`
Mode	Privileged EXEC

Parameter	Description
`address`	IPv6 prefix in IPv6 global address format.
`prefix-length`	IPv6 prefix length value.
`eui64`	Formulate IPv6 address in eui64 format.
`autoconfig`	Configure stateless global address autoconfiguration capability.
`dhcp`	Configure dhcpv6 client protocol.

no network ipv6 address

The command no network ipv6 address removes all configured IPv6 prefixes.

Use this command with the address option to remove the manually configured IPv6 global address on the network port interface.

Use this command with the autoconfig option to disable the stateless global address autoconfiguration on the network port.

Use this command with the dhcp option disables the dhcpv6 client protocol on the network port.

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

network ipv6 gateway

Use this command to configure IPv6 gateway (that is, default routers) information for the network port.

Format	`network ipv6 gateway gateway-address`
Mode	Privileged EXEC

Parameter	Description
gateway-address	Gateway address in IPv6 global or link-local address format.

no network ipv6 gateway

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

Format	`no network ipv6 gateway`
Mode	Privileged EXEC

network ipv6 neighbor

Use this command to manually add IPv6 neighbors to the IPv6 neighbor table for this network port. If an IPv6 neighbor already exists in the neighbor table, the entry is automatically converted to a static entry. Static entries are not modified by the neighbor discovery process. They are, however, treated the same for IPv6 forwarding. Static IPv6 neighbor entries are applied to the kernel stack and to the hardware when the corresponding interface is operationally active.

Format	`network ipv6 neighbor ipv6-address macaddr`
Mode	Privileged EXEC

Parameter	Description
ipv6-address	The IPv6 address of the neighbor or interface.
macaddr	The link-layer address.

no network ipv6 neighbor

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

Format	`no network ipv6 neighbor` *`ipv6-address macaddr`*
Mode	Privileged EXEC

show network ipv6 neighbors

Use this command to display the information about the IPv6 neighbor entries cached on the network port. The information is updated to show the type of the entry.

Default	None
Format	`show network ipv6 neighbors`
Mode	• Privileged EXEC

Column	Meaning
IPv6 Address	The IPv6 address of the neighbor.
MAC Address	The MAC Address of the neighbor.
isRtr	Shows if the neighbor is a router. If TRUE, the neighbor is a router; FALSE it is not a router
Neighbor State	The state of the neighbor cache entry. Possible values are: Incomplete, Reachable, Stale, Delay, Probe, and Unknown
Age	The time in seconds that has elapsed since an entry was added to the cache.
Last Updated	The time in seconds that has elapsed since an entry was added to the cache.
Type	The type of neighbor entry. The type is Static if the entry is manually configured and Dynamic if dynamically resolved.

The following is an example of the command.

```
(Extreme 220) (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
```

show serviceport ipv6 neighbors

Use this command to displays information about the IPv6 neighbor entries cached on the service port. The information is updated to show the type of the entry.

Default	None
Format	`show serviceport ipv6 neighbors`
Mode	Privileged EXEC

Column	Meaning
IPv6 Address	The IPv6 address of the neighbor.
MAC Address	The MAC Address of the neighbor.

Column	Meaning
isRtr	Shows if the neighbor is a router. If TRUE, the neighbor is a router; FALSE it is not a router
Neighbor State	The state of the neighbor cache entry. Possible values are: Incomplete, Reachable, Stale, Delay, Probe, and Unknown
Age	The time in seconds that has elapsed since an entry was added to the cache.
Last Updated	The time in seconds that has elapsed since an entry was added to the cache.
Type	The type of neighbor entry. The type is Static if the entry is manually configured and Dynamic if dynamically resolved.

The following is an example of the command.

```
(Extreme 220) (Routing) #show serviceport ipv6 neighbors
                                                          Neighbor  Age
IPv6 Address                            MAC Address       isRtr State    (Secs)   Type
--------------------------------------- ----------------- ----- --------- ------  --------
FE80::5E26:AFF:FEBD:852C                5c:26:0a:bd:85:2c FALSE Reachable 0       Dynamic
```

ping ipv6

Use this command to determine whether another computer is on the network. Ping provides a synchronous response when initiated from the CLI 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 running on top of TCP/IP. The switch can be pinged from any IP workstation with which the switch is connected through the default VLAN (VLAN 1), as long as there is a physical path between the switch and the workstation. The terminal interface sends three pings to the target station. Use the ipv6-address|hostname parameter to ping an interface by using the global IPv6 address of the interface. Use the optional **`size`** keyword to specify the size of the ping packet. Use the **`outgoing-interface`** option to specify the outgoing interface for a multicast IP/IPv6 ping.

You can utilize the ping or traceroute facilities over the service/network ports when using an IPv6 global address ipv6-global-address|hostname. Any IPv6 global address or gateway assignments to these interfaces will cause IPv6 routes to be installed within the IP stack such that the ping or traceroute request is routed out the service/network port properly. When referencing an IPv6 link-local address, you must also specify the service or network port interface by using the serviceport or network parameter.

Default	• The default count is 1. • The default interval is 3 seconds. • The default size is 0 bytes.
Format	`ping ipv6 {`*`ipv6-global-address`*`|`*`hostname`*` | {interface {`*`unit/slot/port`*` | `*`vlan vlan-id`*` | serviceport | loopback | tunnel | network} `*`link-local-address`*`} [size `*`datagram-size`*`] [outgoing-interface {`*`unit/slot/port`*` | vlan `*`1-4093`*` | serviceport | network}]}`
Mode	• Privileged EXEC • User EXEC

ping ipv6 interface

Use this command to determine whether another computer is on the network. To use the command, configure the switch for network (in-band) connection. The source and target devices must have the ping utility enabled and running on top of TCP/IP. The switch can be pinged from any IP workstation with which the switch is connected through the default VLAN (VLAN 1), as long as there is a physical path between the switch and the workstation. The terminal interface sends three pings to the target station. 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. Use the **outgoing-interface** option to specify the outgoing interface for a multicast IP/IPv6 ping.

Format	`ping ipv6 interface {`*`unit/slot/port`* `| loopback` *`loopback-id`* `| network |serviceport |tunnel` *`tunnel-id`*`} {link-local-address` *`link-local-address`* `|` *`ipv6-address`*`} [size` *`datagram-size`*`] [outgoing-interface {unit/slot/port | vlan 1-4093 | serviceport | network}]`
Modes	• Privileged EXEC • User EXEC

Keyword	Description
size	Use the optional **size** keyword to specify the size of the ping packet.
ipv6-address	The link local IPv6 address of the device you want to query.

Loopback Interface Commands

The commands in this section describe how to create, delete, and manage loopback interfaces. A loopback interface is always expected to be up. This interface can provide the source address for sent packets and can receive both local and remote packets. The loopback interface is typically used by routing protocols.

To assign an IP address to the loopback interface, see ip address on page 506.

interface loopback

Use this command to enter the Interface Config mode for a loopback interface. The range of the loopback ID is 0 to 7.

Format	`interface loopback` *`loopback-id`*
Mode	Global Config

no interface loopback

This command removes the loopback interface and associated configuration parameters for the specified loopback interface.

Format	`no interface loopback` *`loopback-id`*
Mode	Global Config

show interface loopback

This command displays information about configured loopback interfaces.

Format	`show interface loopback [`*`loopback-id`*`]`
Mode	Privileged EXEC

If you do not specify a loopback ID, the following information appears for each loopback interface on the system:

Column	Meaning
Loopback ID	The loopback ID associated with the rest of the information in the row.
Interface	The interface name.
IP Address	The IPv4 address of the interface.

If you specify a loopback ID, the following information appears:

Column	Meaning
Interface Link Status	Shows whether the link is up or down.
IP Address	The IPv4 address of the interface.
MTU size	The maximum transmission size for packets on this interface, in bytes.

IPv6 Routing Commands

This section describes the IPv6 commands used to configure IPv6 on the system and on the interfaces. This section also describes IPv6 management commands and show commands.

show ipv6 nd raguard policy

This command shows the status of IPv6 RA GUARD feature on the switch. It lists the ports/interfaces on which this feature is enabled and the associated device role.

Format	`show ipv6 nd raguard policy`
Mode	Privileged EXEC

Term	Definition
Interface	The port/interface on which this feature is enabled.
Role	The associated device role for the interface.

```
(Extreme 220) # show ipv6 nd raguard policy
Configured Interfaces
           Interface        Role
           ---------------  -------
           Gi1/0/1          Host
```

DHCPv6 Snooping Configuration Commands

This section describes commands used to configure IPv6 *DHCP (Dynamic Host Configuration Protocol)* Snooping.

ipv6 dhcp snooping

Use this command to globally enable IPv6 *DHCP* Snooping.

Default	Disabled
Format	`ipv6 dhcp snooping`
Mode	Global Config

no ipv6 dhcp snooping

Use this command to globally disable IPv6 *DHCP* Snooping.

Format	`no ipv6 dhcp snooping`
Mode	Global Config

ipv6 dhcp snooping vlan

Use this command to enable *DHCP* Snooping on a list of comma-separated VLAN ranges.

Default	Disabled
Format	`ipv6 dhcp snooping vlan` *`vlan-list`*
Mode	Global Config

no ipv6 dhcp snooping vlan

Use this command to disable *DHCP* Snooping on VLANs.

Format	`no ipv6 dhcp snooping vlan` *`vlan-list`*
Mode	Global Config

ipv6 dhcp snooping verify mac-address

Use this command to enable verification of the source MAC address with the client hardware address in the received DCHP message.

Default	Enabled
Format	`ipv6 dhcp snooping verify mac-address`
Mode	Global Config

no ipv6 dhcp snooping verify mac-address

Use this command to disable verification of the source MAC address with the client hardware address.

Format	`no ipv6 dhcp snooping verify mac-address`
Mode	Global Config

ipv6 dhcp snooping binding

Use this command to configure static *DHCP* Snooping binding.

Format	`ipv6 dhcp snooping binding` *`mac-address`* `vlan` *`vlan id ip address`* `interface` *`interface id`*
Mode	Global Config

no ipv6 dhcp snooping binding

Use this command to remove the *DHCP* static entry from the DHCP Snooping database.

Format	`no ipv6 dhcp snooping binding` *`mac-address`*
Mode	Global Config

show ipv6 dhcp snooping

Use this command to display the *DHCP* Snooping global configurations and per port configurations.

Format	`show ipv6 dhcp snooping`
Mode	• Privileged EXEC • User EXEC

Column	Meaning
Interface	The interface for which data is displayed.
Trusted	If it is enabled, DHCP snooping considers the port as trusted. The factory default is disabled.
Log Invalid Pkts	If it is enabled, DHCP snooping application logs invalid packets on the specified interface.

The following example shows CLI display output for the command.

```
(Extreme 220) #show ipv6 dhcp snooping
DHCP snooping is Disabled
DHCP snooping source MAC verification is enabled
DHCP snooping is enabled on the following VLANs:
11 - 30, 40
Interface   Trusted    Log Invalid Pkts
---------   --------   ----------------
0/1          Yes             No
0/2          No             Yes
0/3          No             Yes
0/4          No              No
0/6          No              No
```

show ipv6 dhcp snooping binding

Use this command to display the *DHCP* Snooping binding entries. To restrict the output, use the following options:

- Dynamic: Restrict the output based on DCHP snooping.
- Interface: Restrict the output based on a specific interface.
- Static: Restrict the output based on static entries.
- VLAN: Restrict the output based on VLAN.

Format	`show ipv6 dhcp snooping binding [{static/dynamic}] [interface` *`unit/slot/port`*`] [vlan id]`
Mode	• Privileged EXEC • User EXEC

Column	Meaning
MAC Address	Displays the MAC address for the binding that was added. The MAC address is the key to the binding database.
IPv6 Address	Displays the valid IPv6 address for the binding rule.
VLAN	The VLAN for the binding rule.
Interface	The interface to add a binding into the DHCP snooping interface.
Type	Binding type; statically configured from the CLI or dynamically learned.
Lease (sec)	The remaining lease time for the entry.

The following example shows CLI display output for the command.

```
(Extreme 220) #show ipv6 dhcp snooping binding
Total number of bindings: 2
MAC Address          IPv6 Address  VLAN  Interface  Type
Lease time (Secs)
-----------------  -------------- ----  ---------  ----            ------------------
00:02:B3:06:60:80   2000::1/64     10
 0/1                                                                    86400
00:0F:FE:00:13:04   3000::1/64     10
 0/1                                                                      86400
```

show ipv6 dhcp snooping interfaces

Use this command to show the *DHCP* Snooping status of all interfaces or a specified interface.

Format	`show ipv6 dhcp snooping interfaces [interface unit/slot/port]`
Mode	Privileged EXEC

The following example shows CLI display output for the command.

```
(Extreme 220) #show ipv6 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
(Extreme 220) #show ip dhcp snooping interfaces ethernet 1/0/1
 Interface    Trust State  Rate Limit    Burst Interval
                               (pps)      (seconds)
-----------   -----------   ----------   --------------
    1/0/1      Yes               15              1
```

show ipv6 dhcp snooping statistics

Use this command to list statistics for IPv6 *DHCP* Snooping security violations on untrusted ports.

Format	`show ipv6 dhcp snooping statistics`
Mode	• Privileged EXEC • User EXEC

Column	Meaning
Interface	The IPv6 address of the interface in *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 hardware address mismatch.
Client Ifc Mismatch	Represents the number of DHCP release and Deny messages received on the different ports than learned previously.
DHCP Server Msgs Rec'd	Represents the number of DHCP server messages received on Untrusted ports.

The following example shows CLI display output for the command.

```
 #show ipv6 dhcp snooping statistics
 Interface    MAC Verify   Client Ifc   DHCP Server
               Failures     Mismatch    Msgs Rec'd
-----------   ----------   ----------   -----------
1/0/2                 0            0             0
1/0/3                 0            0             0
1/0/4                 0            0             0
1/0/5                 0            0             0
1/0/6                 0            0             0
1/0/7                 0            0             0
1/0/8                 0            0             0
1/0/9                 0            0             0
1/0/10                0            0             0
1/0/11                0            0             0
```

```
1/0/12                  0               0               0
1/0/13                  0               0               0
1/0/14                  0               0               0
1/0/15                  0               0               0
1/0/16                  0               0               0
1/0/17                  0               0               0
1/0/18                  0               0               0
1/0/19                  0               0               0
1/0/20                  0               0               0
```

clear ipv6 dhcp snooping binding

Use this command to clear all DHCPv6 Snooping bindings on all interfaces or on a specific interface.

Format	`clear ipv6 dhcp snooping binding [interface` *`unit/slot/port`*`]`
Mode	• Privileged EXEC • User EXEC

clear ipv6 dhcp snooping statistics

Use this command to clear all DHCPv6 Snooping statistics.

Format	`clear ipv6 dhcp snooping statistics`
Mode	• Privileged EXEC • User EXEC

8 Quality of Service Commands

This chapter describes the *QoS (Quality of Service)* commands available in the 200 Series CLI.

Caution

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

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

Class of Service Commands

This section describes the commands used to configure and view *CoS (Class of Service)* settings for the switch. The commands in this section allow you to control the priority and transmission rate of traffic.

Note

Commands you issue in the Interface Config mode only affect a single interface. Commands you issue in the Global Config mode affect all interfaces.

classofservice dot1p-mapping

This command maps an 802.1p priority to an internal traffic class. The userpriority values can range from 0-7. The trafficclass values range from 0-6, although the actual number of available traffic classes depends on the platform.

Format	`classofservice dot1p-mapping` *`userpriority trafficclass`*
Modes	• Global Config • Interface Config

no classofservice dot1p-mapping

This command maps each 802.1p priority to its default internal traffic class value.

Format	`no classofservice dot1p-mapping`
Modes	• Global Config • Interface Config

classofservice ip-dscp-mapping

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

The trafficclass values can range from 0-6, although the actual number of available traffic classes depends on the platform.

Format	`classofservice ip-dscp-mapping` *`ipdscp trafficclass`*
Mode	Global Config

no classofservice ip-dscp-mapping

This command maps each IP DSCP value to its default internal traffic class value.

Format	`no classofservice ip-dscp-mapping`
Mode	Global Config

classofservice ip-precedence-mapping

This command maps an IP Precedence value to an internal traffic class for a specific interface. The 0-7 parameter is optional and is only valid on platforms that support independent per-port class of service mappings.

Format	`classofservice ip-precedence-mapping` *`0-7`*
Mode	Global Config

Parameter	Description
0-7	The IP Precedence value.

no classofservice ip-precedence-mapping

This command returns the mapping to its default value.

Format	`no classofservice ip-precedence-mapping`
Mode	Global Config

classofservice trust

This command sets the class of service trust mode of an interface or range of interfaces. You can set the mode to trust one of the Dot1p (802.1p), IP DSCP, or IP Precedence packet markings. You can also set the interface mode to untrusted. If you configure an interface to use Dot1p, the mode does not appear in the output of the show running-config command because Dot1p is the default.

Note
The classofservice trust dot1p command will not be supported in future releases of the software because Dot1p is the default value. Use the no classofservice trust command to set the mode to the default value.

Default	dot1p
Format	`classofservice trust {dot1p | ip-dscp | untrusted}`
Modes	• Global Config • Interface Config

no classofservice trust

This command sets the interface mode to the default value.

Format	`no classofservice trust`
Modes	• Global Config • Interface Config

cos-queue max-bandwidth

This command specifies the maximum 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 maximum bandwidth. The sum of all values entered must not exceed 100.

Format	`cos-queue max-bandwidth` *`bw-0 bw-1 … bw-n`*
Modes	• Global Config • Interface Config

no cos-queue max-bandwidth

This command restores the default for each queue's minimum bandwidth value.

Format	`no cos-queue max-bandwidth`
Modes	• Global Config • Interface Config

cos-queue min-bandwidth

This command specifies the minimum transmission bandwidth guarantee for each interface queue on an interface, a range of interfaces, or all interfaces. 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.

Format	`cos-queue min-bandwidth` *`bw-0 bw-1 … bw-n`*
Modes	• Global Config • Interface Config

no cos-queue min-bandwidth

This command restores the default for each queue's minimum bandwidth value.

Format	`no cos-queue min-bandwidth`
Modes	• Global Config • Interface Config

cos-queue random-detect

This command activates weighted random early discard (WRED) for each specified queue on the interface. Specific WRED parameters are configured using the random-detect queue-parms and the `random-detect exponential-weighting-constant` commands.

Format	`cos-queue random-detect` *`queue-id-1`* `[`*`queue-id-2 … queue-id-n`*`]`
Modes	• Global Config • Interface Config

When specified in Interface Config' mode, this command affects a single interface only, whereas in Global Config mode, it applies to all interfaces.

At least one, but no more than n queue-id values are specified with this command. Duplicate queue-id values are ignored. Each queue-id value ranges from 0 to (n–1), where n is the total number of queues supported per interface. The number n = 7 and corresponds to the number of supported queues (traffic classes).

no cos-queue random-detect

Use this command to disable WRED, thereby restoring the default tail drop operation for the specified queues on the interface.

Format	`no cos-queue random-detect` *`queue-id-1 [queue-id-2 … queue-id-n]`*
Modes	• Global Config • Interface Config

cos-queue strict

This command activates the strict priority scheduler mode for each specified queue for an interface queue on an interface, a range of interfaces, or all interfaces.

Format	`cos-queue strict` *`queue-id-1 [queue-id-2 … queue-id-n]`*
Modes	• Global Config • Interface Config

no cos-queue strict

This command restores the default weighted scheduler mode for each specified queue.

Format	`no cos-queue strict` *`queue-id-1 [queue-id-2 … queue-id-n]`*
Modes	• Global Config • Interface Config

random-detect

This command is used to enable WRED for the interface as a whole, and is only available when per-queue WRED activation control is not supported by the device Specific WRED parameters are configured using the random-detect queue-parms and the `random-detect exponential-weighting-constant` commands.

Format	`random-detect`
Modes	• Global Config • Interface Config

When specified in Interface Config mode, this command affects a single interface only, whereas in Global Config mode, it applies to all interfaces. The Interface Config mode command is only available on platforms that support independent per-port class of service queue configuration.

no random-detect

Use this command to disable WRED, thereby restoring the default tail drop operation for all queues on the interface.

Format	`no random-detect`
Modes	• Global Config • Interface Config

random-detect exponential weighting-constant

This command is used to configure the WRED decay exponent for a *CoS* queue interface.

Format	`random-detect exponential-weighting-constant` *0-15*
Modes	• Global Config • Interface Config

no random-detect exponential-weighting-constant

Use this command to set the WRED decay exponent back to the default.

Format	`no random-detect exponential-weighting-constant`
Modes	• Global Config • Interface Config

random-detect queue-parms

This command is used to configure WRED parameters for each drop precedence level supported by a queue. It is used only when per-COS queue configuration is enabled (using the `cos-queue random-detect` command).

Format	`random-detect queue-parms` *queue-id-1* [*queue-id-2* … *queue-id-n*] **min-thresh** *thresh-prec-1* … *thresh-prec-n* **max-thresh** *thresh-prec-1* … *thresh-prec-n* **drop-probability** *prob-prec-1* … *prob-prec-n*
Modes	• Global Config • Interface Config

Each parameter is specified for each possible drop precedence (color of TCP traffic). The last precedence applies to all non-TCP traffic. For example, in a 3-color system, four of each parameter specified: green TCP, yellow TCP, red TCP, and non-TCP, respectively.

Parameter	Description
min-thresh	The minimum threshold the queue depth (as a percentage) where WRED starts marking and dropping traffic.
max-thresh	The maximum threshold is the queue depth (as a percentage) above which WRED marks / drops all traffic.
drop-probability	The percentage probability that WRED will mark/drop a packet, when the queue depth is at the maximum threshold. (The drop probability increases linearly from 0 just before the minimum threshold, to this value at the maximum threshold, then goes to 100% for larger queue depths).

no random-detect queue-parms

Use this command to set the WRED configuration back to the default.

Format	`no random-detect queue-parms` *`queue-id-1 [queue-id-2 … queue-id-n]`*
Modes	• Global Config • Interface Config

traffic-shape

This command specifies the maximum transmission bandwidth limit for the interface as a whole. The bandwidth values are from 0-100 in increments of 1. You can also specify this value for a range of interfaces or all interfaces. Also known as rate shaping, traffic shaping has the effect of smoothing temporary traffic bursts over time so that the transmitted traffic rate is bounded.

Format	`traffic-shape` *`bandwidth`*
Modes	• Global Config • Interface Config

no traffic-shape

This command restores the interface shaping rate to the default value.

Format	`no traffic-shape`
Modes	• Global Config • Interface Config

show classofservice dot1p-mapping

This command displays the current Dot1p (802.1p) priority mapping to internal traffic classes for a specific interface. 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. For more information, see Voice VLAN Commands on page 336.

Format	`show classofservice dot1p-mapping [unit/slot/port]`
Mode	Privileged EXEC

The following information is displayed for each user priority.

Column	Meaning
User Priority	The 802.1p user priority value.
Traffic Class	The traffic class internal queue identifier to which the user priority value is mapped.

show classofservice ip-dscp-mapping

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

Format	`show classofservice ip-dscp-mapping`
Mode	Privileged EXEC

The following information is repeated for each user priority.

Column	Meaning
IP DSCP	The IP DSCP value.
Traffic Class	The traffic class internal queue identifier to which the IP DSCP value is mapped.

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.

Format	`show classofservice ip-precedence-mapping [unit/slot/port]`
Mode	Privileged EXEC

Column	Meaning
IP Precedence	The IP Precedence value.
Traffic Class	The traffic class internal queue identifier to which the IP Precedence value is mapped.

show classofservice packet-drop-count

This command displays the number of dropped counters for each CoS (Class of Service) egress queue on the specified port.

For 220 Series switches, specify the port name in *unit/slot/port* format.

For 210 Series switches, specify the port name in *slot/port* format.

Format	`show classofservice packet-drop-count` *unit/slot/port* | *slot/port*
Mode	Privileged EXEC

The following shows an example of the command and its output:

```
(Extreme 210) #show classofservice packet-drop-count 0/1

Packets dropped on COS queue 0..................... 0
Packets dropped on COS queue 1..................... 0
Packets dropped on COS queue 2..................... 0
Packets dropped on COS queue 3..................... 0
Packets dropped on COS queue 4..................... 0
Packets dropped on COS queue 5..................... 0
Packets dropped on COS queue 6..................... 0
Packets dropped on COS queue 7..................... 0
Time Since Counters Last Cleared................... 0 day 0 hr 3 min 22 sec
```

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.

Format	`show classofservice trust [`*unit/slot/port*`]`
Mode	Privileged EXEC

Column	Meaning
Class of Service Trust Mode	The the trust mode, which is either Dot1P, IP DSCP, or Untrusted.
Non-IP Traffic Class	(IP DSCP mode only) The traffic class used for non-IP traffic.
Untrusted Traffic Class	(Untrusted mode only) The traffic class used for all untrusted traffic.

show interfaces cos-queue

This command displays the class-of-service queue configuration for the specified interface. 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 class-of-service queue configuration of the interface is displayed. If omitted, the most recent global configuration settings are displayed.

Format	`show interfaces cos-queue [`*unit/slot/port*`]`
Mode	Privileged EXEC

Column	Meaning
Interface Shaping Rate	The global interface shaping rate value.
WRED Decay Exponent	The global WRED decay exponent value.
Queue Id	An interface supports n queues numbered 0 to (n-1). 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.
Maximum Bandwidth	The maximum 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	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.

Column	Meaning
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.
WRED Decay Exponent	The configured WRED decay exponent for a *CoS* queue interface.

show interfaces random-detect

This command displays the global WRED settings for each *CoS* queue. If you specify the unit/slot/port, the command displays the WRED settings for each CoS queue on the specified interface.

Format	`show interfaces random-detect [unit/slot/port]`
Mode	Privileged EXEC

Column	Meaning
Queue ID	An interface supports n queues numbered 0 to (n-1). The specific n value is platform dependent.
WRED Minimum Threshold	The configured minimum threshold the queue depth (as a percentage) where WRED starts marking and dropping traffic.
WRED Maximum Threshold	The configured maximum threshold is the queue depth (as a percentage) above which WRED marks / drops all traffic.
WRED Drop Probability	The configured percentage probability that WRED will mark/drop a packet, when the queue depth is at the maximum threshold. (The drop probability increases linearly from 0 just before the minimum threshold, to this value at the maximum threshold, then goes to 100% for larger queue depths).

show interfaces tail-drop-threshold

This command displays the tail drop threshold information. If you specify the unit/slot/port, the command displays the tail drop threshold information for the specified interface.

Format	`show interfaces tail-drop-threshold [unit/slot/port]`
Mode	Privileged EXEC

Differentiated Services Commands

This section describes the commands used to configure QOS Differentiated Services (DiffServ).

You configure DiffServ in several stages by specifying three DiffServ components:

1 Class

   a Creating and deleting classes.
   b Defining match criteria for a class.

2 Policy

   a Creating and deleting policies
   b Associating classes with a policy
   c Defining policy statements for a policy/class combination

3 Service

   a Adding and removing a policy to/from an inbound interface

The DiffServ class defines the packet filtering criteria. The attributes of a DiffServ policy define the way the switch processes packets. You can define policy attributes on a per-class instance basis. The switch applies these attributes when a match occurs.

Packet processing begins when the switch tests the match criteria for a packet. The switch applies a policy to a packet when it finds a class match within that policy.

The following rules apply when you create a DiffServ class:

- Each class can contain a maximum of one referenced (nested) class
- Class definitions do not support hierarchical service policies

A given class definition can contain a maximum of one reference to another class. You can combine the reference with other match criteria. The referenced class is truly a reference and not a copy since additions to a referenced class affect all classes that reference it. Changes to any class definition currently referenced by any other class must result in valid class definitions for all derived classes, otherwise the switch rejects the change. You can remove a class reference from a class definition.

The only way to remove an individual match criterion from an existing class definition is to delete the class and re-create it.

Note

The mark possibilities for policing include *CoS*, IP DSCP, and IP Precedence. While the latter two are only meaningful for IP packet types, CoS marking is allowed for both IP and non-IP packets, since it updates the 802.1p user priority field contained in the VLAN tag of the layer 2 packet header.

diffserv

This command sets the DiffServ operational mode to active. While disabled, the DiffServ configuration is retained and can be changed, but it is not activated. When enabled, DiffServ services are activated.

Format	`diffserv`
Mode	Global Config

no diffserv

This command sets the DiffServ operational mode to inactive. While disabled, the DiffServ configuration is retained and can be changed, but it is not activated. When enabled, DiffServ services are activated.

Format	`no diffserv`
Mode	Global Config

DiffServ Class Commands

Use the DiffServ class commands to define traffic classification. To classify traffic, you specify Behavior Aggregate (BA), based on DSCP and Multi-Field (MF) classes of traffic (name, match criteria)

This set of commands consists of class creation/deletion and matching, with the class match commands specifying Layer 3, Layer 2, and general match criteria. The class match criteria are also known as class rules, with a class definition consisting of one or more rules to identify the traffic that belongs to the class.

Note

Once you create a class match criterion for a class, you cannot change or delete the criterion. To change or delete a class match criterion, you must delete and re-create the entire class.

The CLI command root is class-map.

class-map

This command defines a DiffServ class of type match-all. When used without any match condition, this command enters the class-map mode. The class-map-name is a case sensitive alphanumeric string from 1 to 31 characters uniquely identifying an existing DiffServ class.

Note
The class-map-name 'default' is reserved and must not be used.

The class type of match-all indicates all of the individual match conditions must be true for a packet to be considered a member of the class. This command may be used without specifying a class type to enter the Class-Map Config mode for an existing DiffServ class.

Note
The optional keyword **ipv4 | ipv6** specifies 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.

Note
The CLI mode is changed to Class-Map Config or Ipv6-Class-Map Config when this command is successfully executed depending on the **ipv4 | ipv6** keyword specified.

Format	`class-map match-all` *`class-map-name`* `[{`**`appiq`** `|` **`ipv4`** `|` **`ipv6`**`}] {ipv4}`
Mode	Global Config

no class-map

This command eliminates an existing DiffServ class. The class-map-name is the name of an existing DiffServ class. (The class name default is reserved and is not allowed here.) This command may be issued at any time; if the class is currently referenced by one or more policies or by any other class, the delete action fails.

Format	`no class-map` *`class-map-name`*
Mode	Global Config

class-map rename

This command changes the name of a DiffServ class. The class-map-name is the name of an existing DiffServ class. The new-class-map-name parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the class.

Default	None
Format	`class-map rename` *`class-map-name new-class-map-name`*
Mode	Global Config

match ethertype

This command adds to the specified class definition a match condition based on the value of the ethertype. The ethertype value is specified as one of the following keywords: appletalk, arp, ibmsna, ipv4, ipv6, ipx, mplsmcast, mplsucast, netbios, novell, pppoe, rarp or as a custom EtherType value in the range of 0x0600-0xFFFF. Use the [not] option to negate the match condition.

Format	`match [not] ethertype {`*`keyword	custom 0x0600-0xFFFF`*`}`
Mode	Class-Map Config Ipv6-Class-Map Config

match any

This command adds to the specified class definition a match condition whereby all packets are considered to belong to the class. Use the [not] option to negate the match condition.

Default	None
Format	`match [not] any`
Mode	Class-Map Config Ipv6-Class-Map Config

match class-map

This command adds to the specified class definition the set of match conditions defined for another class. The refclassname is the name of an existing DiffServ class whose match conditions are being referenced by the specified class definition.

Default	None
Format	`match class-map refclassname`
Mode	Class-Map Config Ipv6-Class-Map Config

Note

The parameters *refclassname* and *class-map-name* can not be the same.

Only one other class may be referenced by a class.

Any attempts to delete the *refclassname* class while the class is still referenced by any *class-map-name* fails.

The combined match criteria of *class-map-name* and *refclassname* must be an allowed combination based on the class type.

Any subsequent changes to the *refclassname* class match criteria must maintain this validity, or the change attempt fails.

The total number of class rules formed by the complete reference class chain (including both predecessor and successor classes) must not exceed a platform-specific maximum. In some cases, each removal of a refclass rule reduces the maximum number of available rules in the class definition by one.

no match class-map

This command removes from the specified class definition the set of match conditions defined for another class. The refclassname is the name of an existing DiffServ class whose match conditions are being referenced by the specified class definition.

Format	`no match class-map refclassname`
Mode	Class-Map Config Ipv6-Class-Map Config

match cos

This command adds to the specified class definition a match condition for the Class of Service value (the only tag in a single tagged packet or the first or outer 802.1Q tag of a double VLAN tagged packet). The value may be from 0 to 7. Use the [not] option to negate the match condition.

Default	None
Format	`match [not] cos 0-7`
Mode	Class-Map Config Ipv6-Class-Map Config

match secondary-cos

This command adds to the specified class definition a match condition for the secondary Class of Service value (the inner 802.1Q tag of a double VLAN tagged packet). The value may be from 0 to 7. Use the [not] option to negate the match condition.

Default	None
Format	`match [not]secondary-cos` *`0-7`*
Mode	Class-Map Config Ipv6-Class-Map Config

match destination-address mac

This command adds to the specified class definition a match condition based on the destination MAC address of a packet. The macaddr parameter is any layer 2 MAC address formatted as six, two-digit hexadecimal numbers separated by colons (for example, 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 (for example, ff:07:23:ff:fe:dc). Use the [not] option to negate the match condition.

Default	None
Format	`match [not] destination-address mac` *`macaddr macmask`*
Mode	Class-Map Config Ipv6-Class-Map Config

match dstip

This command adds to the specified class definition a match condition based on the destination IP address of a packet. The ipaddr parameter specifies an IP address. The ipmask parameter specifies an IP address bit mask and must consist of a contiguous set of leading 1 bits. Use the [not] option to negate the match condition.

Default	None
Format	`match [not] dstip` *`ipaddr ipmask`*
Mode	Class-Map Config

match 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
Format	`match [not] dstip6` *`destination-ipv6-prefix/prefix-length`*
Mode	Ipv6-Class-Map Config

match dstl4port

This command adds to the specified class definition a match condition based on the destination layer 4 port of a packet using a single keyword or numeric notation. To specify the match condition as a single keyword, the value for portkey is one of the supported port name keywords. The currently supported portkey values are: domain, echo, ftp, ftpdata, http, smtp, snmp, telnet, tftp, www. Each of these translates into its equivalent port number. To specify the match condition using a numeric notation, one layer 4 port number is required. The port number is an integer from 0 to 65535. Use the [not] option to negate the match condition.

Default	None
Format	`match [not] dstl4port {`*`portkey`* `|` *`0-65535`*`}`
Mode	Class-Map Config Ipv6-Class-Map Config

match ip dscp

This command adds to the specified class definition a match condition based on the value of the IP DiffServ Code Point (DSCP) field in a packet, which is defined as the high-order six bits of the Service Type octet in the IP header (the low-order two bits are not checked).

The dscpval value is specified as either an integer from 0 to 63, or symbolically through one of the following keywords: af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, ef. Use the [not] option to negate the match condition.

Note
The ip dscp, ip precedence, and ip tos match conditions are alternative ways to specify a match criterion for the same Service Type field in the IP header, but with a slightly different user notation.

Default	None
Format	`match [not] ip dscp` *`dscpval`*
Mode	Class-Map Config Ipv6-Class-Map Config

match ip precedence

This command adds to the specified class definition a match condition based on the value of the IP Precedence field in a packet, which is defined as the high-order three bits of the Service Type octet in the IP header (the low-order five bits are not checked). The precedence value is an integer from 0 to 7. Use the [not] option to negate the match condition.

Note
The IP DSCP, IP Precedence, and IP ToS match conditions are alternative ways to specify a match criterion for the same Service Type field in the IP header, but with a slightly different user notation.

Default	None
Format	`match [not] ip precedence 0-7`
Mode	Class-Map Config

match ip tos

This command adds to the specified class definition a match condition based on the value of the IP TOS field in a packet, which is defined as all eight bits of the Service Type octet in the IP header. The value of tosbits is a two-digit hexadecimal number from 00 to ff. The value of tosmask is a two-digit hexadecimal number from 00 to ff. The tosmask denotes the bit positions in tosbits that are used for comparison against the IP TOS field in a packet. For example, to check for an IP TOS value having bits 7 and 5 set and bit 1 clear, where bit 7 is most significant, use a tosbits value of a0 (hex) and a tosmask of a2 (hex). Use the [not] option to negate the match condition.

Note
The IP DSCP, IP Precedence, and IP ToS match conditions are alternative ways to specify a match criterion for the same Service Type field in the IP header, but with a slightly different user notation.

Note
This “free form” version of the IP DSCP/Precedence/TOS match specification gives the user complete control when specifying which bits of the IP Service Type field are checked.

Default	None
Format	`match [not] ip tos tosbits tosmask`
Mode	Class-Map Config

match ip6flowlbl

Use this command to enter an IPv6 flow label value. Use the [not] option to negate the match condition.

Default	None
Format	`match [not] ip6flowlbl label 0-1048575`
Mode	IPv6-Class-Map Config

match protocol

This command adds to the specified class definition a match condition based on the value of the IP Protocol field in a packet using a single keyword notation or a numeric value notation.

To specify the match condition using a single keyword notation, the value for protocol-name is one of the supported protocol name keywords. The currently supported values are: icmp, igmp, ip, tcp, udp. A value of ip matches all protocol number values.

To specify the match condition using a numeric value notation, the protocol number is a standard value assigned by IANA and is interpreted as an integer from 0 to 255. Use the [not] option to negate the match condition.

Note
This command does not validate the protocol number value against the current list defined by IANA.

Default	None
Format	`match [not] protocol {protocol-name | 0-255}`
Mode	Class-Map Config Ipv6-Class-Map Config

match signature

This command maps the available signatures from the rules file to the AppIQ class. When the appiq class is created, this menu displays an index number and its signature pattern. A single signature can be mapped using a number or multiple signatures can be selected and mapped to a class. Using this command without an index value maps all the available signatures to the same class.

Default	None
Format	`match signature [StartIndex-EndIndex]`
Mode	Class-Map Config

match srcip

This command adds to the specified class definition a match condition based on the source IP address of a packet. The ipaddr parameter specifies an IP address. The ipmask parameter specifies an IP address bit mask and must consist of a contiguous set of leading 1 bits. Use the [not] option to negate the match condition.

Default	None
Format	`match [not] srcip ipaddr ipmask`
Mode	Class-Map Config

match 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
Format	`match [not] srcip6 source-ipv6-prefix/prefix-length`
Mode	Ipv6-Class-Map Config

match srcl4port

This command adds to the specified class definition a match condition based on the source layer 4 port of a packet using a single keyword or numeric notation. To specify the match condition as a single keyword notation, the value for portkey is one of the supported port name keywords (listed here). The currently supported portkey values are: domain, echo, ftp, ftpdata, http, smtp, snmp, telnet, tftp, www. Each of these translates into its equivalent port number, which is used as both the start and end of a port range.

To specify the match condition as a numeric value, one layer 4 port number is required. The port number is an integer from 0 to 65535. Use the [not] option to negate the match condition.

Default	None
Format	`match [not] srcl4port {`*`portkey`* `|` *`0-65535`*`}`
Mode	Class-Map Config Ipv6-Class-Map Config

match 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
Format	`match src port {`*`portstart-portend`* `|` *`portvalue`*`}`
Mode	Class-Map Config

match vlan

This command adds to the specified class definition a match condition based on the value of the layer 2 VLAN Identifier field (the only tag in a single tagged packet or the first or outer tag of a double VLAN tagged packet). The VLAN ID is an integer from 0 to 4093. Use the [not] option to negate the match condition.

Default	None
Format	`match [not] vlan` *`0-4093`*
Mode	Class-Map Config Ipv6-Class-Map Config

match secondary-vlan

This command adds to the specified class definition a match condition based on the value of the layer 2 secondary VLAN Identifier field (the inner 802.1Q tag of a double VLAN tagged packet). The secondary VLAN ID is an integer from 0 to 4093. Use the [not] option to negate the match condition.

Default	None
Format	`match [not] secondary-vlan` *`0-4093`*
Mode	Class-Map Config Ipv6-Class-Map Config

DiffServ Policy Commands

Use the DiffServ policy commands to specify traffic conditioning actions, such as policing and marking, to apply to traffic classes

Use the policy commands to associate a traffic class that you define by using the class command set with one or more *QoS* policy attributes. Assign the class/policy association to an interface to form a service. Specify the policy name when you create the policy.

Each traffic class defines a particular treatment for packets that match the class definition. You can associate multiple traffic classes with a single policy. When a packet satisfies the conditions of more than one class, preference is based on the order in which you add the classes to the policy. The first class you add has the highest precedence.

This set of commands consists of policy creation/deletion, class addition/removal, and individual policy attributes.

Note

The only way to remove an individual policy attribute from a class instance within a policy is to remove the class instance and re-add it to the policy. The values associated with an existing policy attribute can be changed without removing the class instance.

The CLI command root is policy-map.

assign-queue

This command modifies the queue id to which the associated traffic stream is assigned. The queueid is an integer from 0 to n-1, where n is the number of egress queues supported by the device.

Format	`assign-queue` *`queueid`*
Mode	Policy-Class-Map Config
Incompatibilities	Drop

drop

This command specifies that all packets for the associated traffic stream are to be dropped at ingress.

Format	`drop`
Mode	Policy-Class-Map Config
Incompatibilities	Assign Queue, Mark (all forms), Mirror, Police, Redirect

conform-color

Use this command to enable color-aware traffic policing and define the conform-color class map. Used in conjunction with the police command where the fields for the conform level are specified. The class-map-name parameter is the name of an existing DiffServ class map.

Note
This command may only be used after specifying a police command for the policy-class instance.

Format	`conform-color` *`class-map-name`*
Mode	Policy-Class-Map Config

class

This command creates an instance of a class definition within the specified policy for the purpose of defining treatment of the traffic class through subsequent policy attribute statements. The classname is the name of an existing DiffServ class.

Note
This command causes the specified policy to create a reference to the class definition.

Note
The CLI mode is changed to Policy-Class-Map Config when this command is successfully executed.

Format	`class` *`classname`*
Mode	Policy-Map Config

no class

This command deletes the instance of a particular class and its defined treatment from the specified policy. classname is the names of an existing DiffServ class.

Note
This command removes the reference to the class definition for the specified policy.

Format	`no class` *`classname`*
Mode	Policy-Map Config

mark cos

This command marks all packets for the associated traffic stream with the specified *CoS* value in the priority field of the 802.1p header (the only tag in a single tagged packet or the first or outer 802.1Q tag of a double VLAN tagged packet). If the packet does not already contain this header, one is inserted. The CoS value is an integer from 0 to 7.

Default	1
Format	`mark-cos 0-7`
Mode	Policy-Class-Map Config
Incompatibilities	Drop, Mark IP DSCP, IP Precedence, Police

mark secondary-cos

This command marks the outer VLAN tags in the packets for the associated traffic stream as secondary *CoS*.

Default	1
Format	`mark secondary-cos 0-7`
Mode	Policy-Class-Map Config
Incompatibilities	Drop, Mark IP DSCP, IP Precedence, Police

mark cos-as-sec-cos

This command marks outer VLAN tag priority bits of all packets as the inner VLAN tag priority, marking *CoS* as Secondary CoS. This essentially means that the inner VLAN tag CoS is copied to the outer VLAN tag CoS.

Format	`mark-cos-as-sec-cos`
Mode	Policy-Class-Map Config
Incompatibilities	Drop, Mark IP DSCP, IP Precedence, Police

mark ip-dscp

This command marks all packets for the associated traffic stream with the specified IP DSCP value.

The dscpval value is specified as either an integer from 0 to 63, or symbolically through one of the following keywords: af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, ef.

Format	`mark ip-dscp dscpval`
Mode	Policy-Class-Map Config
Incompatibilities	Drop, Mark *CoS*, Mark IP Precedence, Police

mark ip-precedence

This command marks all packets for the associated traffic stream with the specified IP Precedence value. The IP Precedence value is an integer from 0 to 7.

Note
This command may not be used on IPv6 classes. IPv6 does not have a precedence field.

Format	`mark ip-precedence 0-7`
Mode	Policy-Class-Map Config
Incompatibilities	Drop, Mark CoS, Mark IP Precedence, Police
Policy Type	In

police-simple

This command is used to establish the traffic policing style for the specified class. The simple form of the **police** command uses a single data rate and burst size, resulting in two outcomes: conform and violate. The conforming data rate is specified in kilobits-per-second (Kbps) and is an integer from 1 to 4294967295. The conforming burst size is specified in kilobytes (KB) and is an integer from 1 to 128.

For each outcome, the only possible actions are drop, set-cos-as-sec-cos, set-cos-transmit, set-sec-cos-transmit, set-dscp-transmit, set-prec-transmit, or transmit. In this simple form of the **police** command, the conform action defaults to transmit and the violate action defaults to drop. These actions can be set with this command once the style has been configured.

For set-dscp-transmit, a dscpval value is required and is specified as either an integer from 0 to 63, or symbolically through one of the following keywords: af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, ef.

For set-prec-transmit, an IP Precedence value is required and is specified as an integer from 0-7.

For set-cos-transmit an 802.1p priority value is required and is specified as an integer from 0-7.

Format	`police-simple {1-4294967295 1-128 conform-action {drop| set-cos-as-sec-cos | set-cos-transmit 0-7 | set-sec-cos-transmit 0-7 | set-prec-transmit 0-7 | set-dscp-transmit 0-63 | transmit} [violate-action {drop | set-cos-as-sec-cos | set-cos-transmit 0-7 | set-sec-cos-transmit 0-7 | set-prec-transmit 0-7 | set-dscp-transmit 0-63 | transmit}]}`
Mode	Policy-Class-Map Config
Incompatibilities	Drop, Mark (all forms)

police-single-rate

This command is the single-rate form of the **police** command and is used to establish the traffic policing style for the specified class. For each outcome, the only possible actions are drop, set-cos-as-sec-cost, set-cos-transmit, set-sec-cos-transmit, set-dscp-transmit, set-prec-transmit, or transmit. In this single-rate form of the **police** command, the conform action defaults to send, the exceed action defaults to drop, and the violate action defaults to drop. These actions can be set with this command once the style has been configured.

Format	`police-single-rate {1-4294967295 1-128 1-128 conform-action {drop| set-cos-as-sec-cos | set-cos-transmit 0-7 | set-sec-cos-transmit 0-7 | set-prec-transmit 0-7 | set-dscp-transmit 0-63 | transmit} exceed-action {drop | set-cos-as-sec-cos | set-cos-transmit 0-7 | set-sec-cos-transmit 0-7 | set-prec-transmit 0-7 | set-dscp-transmit 0-63 | transmit} [violate-action {drop | set-cos-as-sec-cos-transmit | set-cos-transmit 0-7 | set-sec-cos-transmit 0-7 | set-prec-transmit 0-7 | set-dscp-transmit 0-63 | transmit}]}`
Mode	Policy-Class-Map Config

police-two-rate

This command is the two-rate form of the **police** command and is used to establish the traffic policing style for the specified class. For each outcome, the only possible actions are drop, set-cos-as-sec-cos, set-cos-transmit, set-sec-cos-transmit, set-dscp-transmit, set-prec-transmit, or transmit. In this two-rate form of the **police** command, the conform action defaults to send, the exceed action defaults to drop, and the violate action defaults to drop. These actions can be set with this command once the style has been configured.

Format	`police-two-rate {1-4294967295 conform-action {drop | set-cos-as-sec-cos | set-cos-transmit 0-7 | set-sec-cos-transmit 0-7 | set-prec-transmit 0-7 | set-dscp-transmit 0-63 | transmit} exceed-action {drop | set-cos-as-sec-cos | set-cos-transmit 0-7 | set-sec-cos-transmit 0-7 | set-prec-transmit 0-7 | set-dscp-transmit 0-63 | transmit} [violate-action {drop | set-cos-as-sec-cos | set-cos-transmit 0-7 | set-sec-cos-transmit 0-7 | set-prec-transmit 0-7 | set-dscp-transmit 0-63 | transmit}]}`
Mode	Policy-Class-Map Config

policy-map

This command establishes a new DiffServ policy. The policyname parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the policy. The type of policy is specific

to the inbound traffic direction as indicated by the in parameter, or the outbound traffic direction as indicated by the out parameter, respectively.

Note
The CLI mode is changed to Policy-Map Config when this command is successfully executed.

Format	`policy-map` *`policyname`* `{in|out}`
Mode	Global Config

no policy-map

This command eliminates an existing DiffServ policy. The policyname parameter is the name of an existing DiffServ policy. This command may be issued at any time. If the policy is currently referenced by one or more interface service attachments, this delete attempt fails.

Format	`no policy-map` *`policyname`*
Mode	Global Config

policy-map rename

This command changes the name of a DiffServ policy. The policyname 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.

Format	`policy-map rename` *`policyname newpolicyname`*
Mode	Global Config

DiffServ Service Commands

Use the DiffServ service commands to assign a DiffServ traffic conditioning policy, which you specified by using the policy commands, to an interface in the incoming direction. The service commands attach a defined policy to a directional interface. You can assign only one policy at any one time to an interface in the inbound direction. DiffServ is not used in the outbound direction.

This set of commands consists of service addition/removal.

The CLI command root is service-policy.

service-policy

This command attaches a policy to an interface in the inbound direction as indicated by the in parameter, or the outbound direction as indicated by the out parameter, respectively. The policyname

parameter is the name of an existing DiffServ policy. This command causes a service to create a reference to the policy.

Note
This command effectively enables DiffServ on an interface in the inbound direction. There is no separate interface administrative 'mode' command for DiffServ.

Note
This command fails if any attributes within the policy definition exceed the capabilities of the interface. Once a policy is successfully attached to an interface, any attempt to change the policy definition, that would result in a violation of the interface capabilities, causes the policy change attempt to fail.

Format	`service-policy {in|out} policymapname`
Modes	• Global Config • Interface Config

Note
Each interface can have one policy attached.

no service-policy

This command detaches a policy from an interface in the inbound direction as indicated by the in parameter, or the outbound direction as indicated by the out parameter, respectively. The policyname parameter is the name of an existing DiffServ policy.

Note
This command causes a service to remove its reference to the policy. This command effectively disables DiffServ on an interface in the inbound direction or an interface in the outbound direction. There is no separate interface administrative 'mode' command for DiffServ.

Format	`no service-policy {in|out} policymapname`
Modes	• Global Config • Interface Config

DiffServ Show Commands

Use the DiffServ show commands to display configuration and status information for classes, policies, and services. You can display DiffServ information in summary or detailed formats. The status information is only shown when the DiffServ administrative mode is enabled.

show class-map

This command displays all configuration information for the specified class. The class-name is the name of an existing DiffServ class.

Format	`show class-map` *`class-name`*
Modes	• Privileged EXEC • User EXEC

If the class-name is specified the following fields are displayed:

Column	Meaning
Class Name	The name of this class.
Class Type	A class type of all means every match criterion defined for the class is evaluated simultaneously and must all be true to indicate a class match.
Class Layer3 Protocol	The Layer 3 protocol for this class. Possible values are IPv4 and IPv6value 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:

Column	Meaning
Class Name	The name of this class. (Note that the order in which classes are displayed is not necessarily the same order in which they were created.)
Class Type	A class type of all means every match criterion defined for the class is evaluated simultaneously and must all be true to indicate a class match.
Ref Class Name	The name of an existing DiffServ class whose match conditions are being referenced by the specified class definition.

show diffserv

This command displays the DiffServ General Status Group information, which includes the current administrative mode setting as well as the current and maximum number of rows in each of the main DiffServ private MIB tables. This command takes no options.

Format	`show diffserv`
Mode	Privileged EXEC

Column	Meaning
DiffServ Admin mode	The current value of the DiffServ administrative mode.
Class Table Size Current/Max	The current and maximum number of entries (rows) in the Class Table.
Class Rule Table Size Current/Max	The current and maximum number of entries (rows) in the Class Rule Table.
Policy Table Size Current/Max	The current and maximum number of entries (rows) in the Policy Table.

Column	Meaning
Policy Instance Table Size Current/Max	The current and maximum number of entries (rows) in the Policy Instance Table.
Policy Instance Table Max Current/Max	The current and maximum number of entries (rows) for the Policy Instance Table.
Policy Attribute Table Max Current/Max	The current and maximum number of entries (rows) for the Policy Attribute Table.
Service Table Size Current/Max	The current and maximum number of entries (rows) in the Service Table.

show policy-map

This command displays all configuration information for the specified policy. The policyname is the name of an existing DiffServ policy.

Format	`show policy-map` *`[policyname]`*
Mode	Privileged EXEC

If the Policy Name is specified the following fields are displayed:

Column	Meaning
Policy Name	The name of this policy.
Policy Type	The policy type (only inbound policy definitions are supported for this platform.)
Class Members	The class that is a member of the policy.

The following information is repeated for each class associated with this policy (only those policy attributes actually configured are displayed):

Column	Meaning
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.

Column	Meaning
Drop	Drop a packet upon arrival. This is useful for emulating access control list operation using DiffServ, especially when DiffServ and *ACL (Access Control List)* 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 you can 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 (that is, inner) tag of a double-tagged packet.
Mark IP DSCP	The mark/re-mark value used as the DSCP for traffic matching this class. This is not displayed if mark ip description is not specified.
Mark IP Precedence	The mark/re-mark value used as the IP Precedence for traffic matching this class. This is not displayed if mark ip precedence is not specified.
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	Guarantees a committed rate for transmission, but also transmits excess traffic bursts up to a user-specified peak rate, with the understanding that a downstream network element (such as the next hop's policer) might drop this excess traffic. Traffic is held in queue until it is transmitted or dropped (per type of queue depth management.) Peak rate shaping can be configured for the outgoing transmission stream for an AF (Assured Forwarding) 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 (for example, a token bucket rate limiter) Traffic that exceeds this limit is discarded.
Policing Style	The style of policing, if any, used (simple).

If the Policy Name is not specified this command displays a list of all defined DiffServ policies. The following fields are displayed:

Column	Meaning
Policy Name	The name of this policy. (The order in which the policies are displayed is not necessarily the same order in which they were created.)
Policy Type	The policy type (Only inbound is supported).
Class Members	List of all class names associated with this policy.

The following example shows CLI display output including the mark-cos-as-sec-cos option specified in the policy action.

```
(Extreme 220) (Routing) #show policy-map p1
Policy Name..................................... p1
```

```
Policy Type..................................... In
Class Name...................................... c1
Mark CoS as Secondary CoS....................... Yes
```

The following example shows CLI display output including the mark-cos-as-sec-cos action used in the policing (simple-police, police-single-rate, police two-rate) command.

```
(Extreme 220) (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
```

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.

Format	`show diffserv service` *`unit/slot/port`* `in`
Mode	Privileged EXEC

Column	Meaning
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).

show diffserv service brief

This command displays all interfaces in the system to which a DiffServ policy has been attached. The inbound direction parameter is optional.

Format	`show diffserv service brief [in]`
Mode	Privileged EXEC

Column	Meaning
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):

Column	Meaning
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.

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. Instead of unit/slot/port, lag lag-intf-num can be used as an alternate way to specify the *LAG (Link Aggregation Group)* interface. lag lag-intf-num can also be used to specify the LAG interface where lag-intf-num is the LAG port number.

Note
This command is only allowed while the DiffServ administrative mode is enabled.

Format	`show policy-map interface` *`unit/slot/port`* `[in]`
Mode	Privileged EXEC

Column	Meaning
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.

The following information is repeated for each class instance within this policy:

Column	Meaning
Class Name	The name of this class instance.
In Discarded Packets	A count of the packets discarded for this class instance for any reason due to DiffServ treatment of the traffic class.

show service-policy

This command displays a summary of policy-oriented statistics information for all interfaces in the specified direction.

Format	show service-policy in
Mode	Privileged EXEC

The following information is repeated for each interface and direction (only those interfaces configured with an attached policy are shown):

Column	Meaning
Interface	*unit/slot/port*
Operational Status	The current operational status of this DiffServ service interface.
Policy Name	The name of the policy attached to the interface.

MAC Access Control List Commands

This section describes the commands used to configure MAC *ACL* settings. MAC ACLs ensure that only authorized users have access to specific resources and block any unwarranted attempts to reach network resources.

The following rules apply to MAC ACLs:

- The maximum number of ACLs you can create is hardware dependent. The limit applies to all ACLs, regardless of type.
- The system supports only Ethernet II frame types.
- The maximum number of rules per MAC ACL is hardware dependent.

mac access-list extended

This command creates a MAC *ACL* identified by name, consisting of classification fields defined for the Layer 2 header of an Ethernet frame. The name parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the MAC access list. The rate-limit attribute configures the committed rate and the committed burst size.

If a MAC ACL by this name already exists, this command enters Mac-Access-List config mode to allow updating the existing MAC ACL.

Note
The CLI mode changes to Mac-Access-List Config mode when you successfully execute this command.

Format	mac access-list extended *name*
Mode	Global Config

no mac access-list extended

This command deletes a MAC *ACL* identified by name from the system.

Format	no mac access-list extended *name*
Mode	Global Config

mac access-list extended rename

This command changes the name of a MAC *ACL*. The name parameter is the name of an existing MAC ACL. The newname parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the MAC access list.

This command fails if a MAC ACL by the name newname already exists.

Format	`mac access-list extended rename name newname`
Mode	Global Config

mac access-list resequence

Use this command to renumber the sequence numbers of the entries for specified MAC access list with the given increment value starting from a particular sequence number. The command is used to edit the sequence numbers of *ACL* rules in the ACL and change the order in which entries are applied. This command is not saved in startup configuration and is not displayed in running configuration.

Note
If the generated sequence number exceeds the maximum sequence number, the ACL rule creation fails and an informational message is displayed.

Default	10
Format	`mac access-list resequence {name| id } starting-sequence-number increment`
Mode	Global Config

Parameter	Description
starting-sequence-number	The sequence number from which to start. The range is 1–2147483647. The default is 10.
increment	The amount to increment. The range is 1–2147483647. The default is 10.

{deny | permit} (MAC ACL)

This command creates a new rule for the current MAC access list. A rule may either deny or permit traffic according to the specified classification fields. At a minimum, the source and destination MAC value must be specified, each of which may be substituted using the keyword any to indicate a match on any value in that field. The remaining command parameters are all optional, but the most frequently used parameters appear in the same relative order as shown in the command format.

Format	[*sequence-number*] {deny|permit} {*srcmac* | any} {*dstmac* | any} [*ethertypekey* | *0x0600-0xFFFF*] [vlan {eq *0-4095*}] [cos *0-7*] [[log] [time-range time-range-name] [assign-queue *queue-id*]] [*unit/slot/port*][rate-limit rate burst-size]
Mode	Mac-Access-List Config

Note
An implicit deny all MAC rule always terminates the access list.

The sequence-number specifies the sequence number for the ACL rule. The sequence number is specified by the user or is generated by device.

If a sequence number is not specified for the rule, a sequence number that is 10 greater than the last sequence number in ACL is used and this rule is placed in the end of the list. If this is the first ACL rule in the given ACL, a sequence number of 10 is assigned. If the calculated sequence number exceeds the maximum sequence number value, the ACL rule creation fails. A rule cannot be created that duplicates an already existing one and a rule cannot be configured with a sequence number that is already used for another rule.

For example, if user adds new ACL rule to ACL without specifying a sequence number, it is placed at the bottom of the list. By changing the sequence number, the user can move the ACL rule to a different position in the ACL.

The Ethertype may be specified as either a keyword or a four-digit hexadecimal value from 0x0600-0xFFFF. The currently supported ethertypekey values are: appletalk, arp, ibmsna, ipv4, ipv6, ipx, mplsmcast, mplsucast, netbios, novell, pppoe, rarp. Each of these translates into its equivalent Ethertype value(s).

Table 13: Ethertype Keyword and 4-digit Hexadecimal Value

Ethertype Keyword	Corresponding Value
appletalk	0x809B
arp	0x0806
ibmsna	0x80D5
ipv4	0x0800
ipv6	0x86DD
ipx	0x8037
mplsmcast	0x8848
mplsucast	0x8847
netbios	0x8191
novell	0x8137, 0x8138
pppoe	0x8863, 0x8864
rarp	0x8035

The vlan and cos parameters refer to the VLAN identifier and 802.1p user priority fields, respectively, of the VLAN tag. For packets containing a double VLAN tag, this is the first (or outer) tag.

The time-range parameter allows imposing time limitation on the MAC ACL rule as defined by the parameter time-range-name. If a time range with the specified name does not exist and the MAC ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied immediately. If a time range with specified name exists and the MAC ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied when the time-range with specified name becomes active. The ACL rule is removed when the time-range with specified name becomes inactive. For information about configuring time ranges, see Time Range Commands for Time-Based ACLs on page 653.

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.

Note
The special command form {deny | permit} any any is used to match all Ethernet layer 2 packets, and is the equivalent of the IP access list “match every” rule.

The permit command’s optional attribute rate-limit allows you to permit only the allowed rate of traffic as per the configured rate in kbps, and burst-size in kbytes.

The following shows an example of the command.

```
(Extreme 220) (Config) #mac access-list extended mac1
(Extreme 220) (Config-mac-access-list)#permit 00:00:00:00:aa:bb ff:ff:ff:ff:00:00 any rate-
limit 32 16
(Extreme 220) (Config-mac-access-list)#exit
```

no sequence-number

Use this command to remove the *ACL* rule with the specified sequence number from the ACL.

Format	`no sequence-number`
Mode	MAC-Access-List Config

mac access-group

This command either attaches a specific MAC *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.

Note
The keyword control-plane is only available in Global Config mode.

Note
You should be aware that the *out* option may or may not be available, depending on the platform.

Format	`mac access-group` *`name`* `{{`*`control-plane`*`|in|out}` **`vlan`** `vlan-id {in|out}} [sequence 1-4294967295]`
Modes	• Global Config • Interface Config

Parameter	Description
name	The name of the Access Control List.
sequence	A optional sequence number that indicates the order of this IP access list relative to the other IP access lists already assigned to this interface and direction. The range is 1 to 4294967295.
vlan-id	A VLAN ID associated with a specific IP ACL in a given direction.

The following shows an example of the command.

```
(Extreme 220) (Config)#mac access-group mac1 control-plane
```

no mac access-group

This command removes a MAC *ACL* identified by name from the interface in a given direction.

Format	`no mac access-group` *`name`* `{{`*`control-plane`*`|in|out} vlan vlan-id {in|out}}`
Modes	• Global Config • Interface Config

The following shows an example of the command.

```
(Extreme 220) (Routing)(Config)#no mac access-group mac1 control-plane
```

remark

This command adds a new comment to the *ACL* rule.

Use the remark keyword to add comments (remarks) to ACL rule entries belonging to an IPv4, IPv6, MAC, or ARP ACL. Up to L7_ACL_MAX_RULES_PER_LIST*10 remarks per ACL and up to 10 remarks per ACL rule can be configured. Also, up to L7_ACL_MAX_RULES*2 remarks for all QOS ACLs(IPv4/IPv6/MAC) for device can be configured. The total length of the remark cannot exceed 100 characters. A remark can contain characters in the range A-Z, a-z, 0-9, and special characters like space, hyphen, underscore. Remarks are associated to the ACL rule that is immediately created after the remarks are created. If the ACL rule is removed, the associated remarks are also deleted. Remarks are shown only in show running-config and are not displayed in show ip access-lists.

Remarks can only be added before creating the rule. If a user creates up to 10 remarks, each of them is linked to the next created rule.

Default	None
Format	`remark comment`
Mode	• IPv4-Access-List Config • IPv6-Access-List-Config • MAC-Access-List Config • ARP-Access-List Config

```
(Config)#arp access-list new
(Config-arp-access-list)#remark "test1"
(Config-arp-access-list)#permit ip host 1.1.1.1 mac host 00:01:02:03:04:05
(Config-arp-access-list)#remark "test1"
(Config-arp-access-list)#remark "test2"
(Config-arp-access-list)#remark "test3"
(Config-arp-access-list)#permit ip host 1.1.1.2 mac host 00:03:04:05:06:07
(Config-arp-access-list)#permit ip host 2.1.1.2 mac host 00:03:04:05:06:08
(Config-arp-access-list)#remark "test4"
(Config-arp-access-list)#remark "test5"
(Config-arp-access-list)#permit ip host 2.1.1.3 mac host 00:03:04:05:06:01
```

no remark

Use this command to remove a remark from an *ACL* access-list.

When the first occurrence of the remark in ACL is found, the remark is deleted. Repeated execution of this command with the same remark removes the remark from the next ACL rule that has the remark associated with it (if there is any rule configured with the same remark). If there are no more rules with this remark, an error message is displayed

If there is no such remark associated with any rule and such remark is among not associated remarks, it is removed.

Default	None
Format	`no remark comment`
Mode	• IPv4-Access-List Config • IPv6-Access-List-Config • MAC-Access-List Config • ARP-Access-List Config

show mac access-lists

This command displays summary information for all Mac Access lists and *ACL* rule hit count of packets matching the configured ACL rule within an ACL. This counter value rolls-over on reaching the maximum value. There is a dedicated counter for each ACL rule. ACL counters do not interact with PBR counters.

For ACL with multiple rules, once a match occurs at any one specific rule, counters associated with this rule only get incremented (for example, consider an ACL with three rules, after matching rule two, counters for rule three would not be incremented).

For ACL counters, If an ACL rule is configured without RATE-LIMIT, the counter value is count of forwarded/discarded packets. (For example: For a burst of 100 packets, the Counter value is 100).

If the ACL rule is configured with RATE LIMIT, the counter value is the MATCHED packet count. If the sent traffic rate exceeds the configured limit, the counters still display matched packet count (despite getting dropped beyond the configured limit since match criteria is met) which would equal the sent rate. For example, if rate limit is set to 10 kbps and 'matching' traffic is sent at 100 kbps, counters reflect a 100 kbps value. If the sent traffic rate is less than the configured limit, counters display only the matched packet count. Either way, only the matched packet count is reflected in the counters, irrespective of whether they get dropped or forwarded. ACL counters do not interact with diffserv policies.

Use the access list name to display detailed information of a specific MAC ACL.

Note
The command output varies based on the match criteria configured within the rules of an ACL.

Format	`show mac access-lists [name]`
Mode	Privileged EXEC

Column	Meaning
Rule Number	The ordered rule number identifier defined within the MAC ACL.
Action	The action associated with each rule. The possible values are Permit or Deny.
Source MAC Address	The source MAC address for this rule.
Source MAC Mask	The source MAC mask for this rule.
Committed Rate	The committed rate defined by the rate-limit attribute.
Committed Burst Size	The committed burst size defined by the rate-limit attribute.
Destination MAC Address	The destination MAC address for this rule.
Ethertype	The Ethertype keyword or custom value for this rule.
VLAN ID	The VLAN identifier value or range for this rule.
COS	The COS (802.1p) value for this rule.
Log	Displays when you enable logging for the rule.
Assign Queue	The queue identifier to which packets matching this rule are assigned.

Column	Meaning
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.
ACL Hit Count	The ACL rule hit count of packets matching the configured ACL rule within an ACL.

The following example shows CLI display output for the command.

```
(Extreme 220) (Routing) #show mac access-lists mac1
ACL Name: mac1
Outbound Interface(s): control-plane
Sequence Number: 10
Action.............................permit
Source MAC Address................. 00:00:00:00:AA:BB
Source MAC Mask....................FF:FF:FF:FF:00:00
Committed Rate.....................32
Committed Burst Size...............16
ACL hit count .....................0
Sequence Number: 25
Action.............................permit
Source MAC Address................. 00:00:00:00:AA:BB
Source MAC Mask....................FF:FF:FF:FF:00:00
Destination MAC Address........... 01:80:C2:00:00:00
Destination MAC Mask...............00:00:00:FF:FF:FF
Ethertype..........................ipv6
VLAN...............................36
CoS Value..........................7
Assign Queue.......................4
Redirect Interface.................0/34
Committed Rate.....................32
Committed Burst Size...............16
ACL hit count .....................0
```

IP Access Control List Commands

This section describes the commands used to configure IP *ACL* settings. IP ACLs ensure that only authorized users have access to specific resources and block any unwarranted attempts to reach network resources.

The following rules apply to IP ACLs:

- 200 Series software does not support IP ACL configuration for IP packet fragments.
- The maximum number of ACLs you can create is hardware dependent. The limit applies to all ACLs, regardless of type.
- The maximum number of rules per IP ACL is hardware dependent.
- Wildcard masking for ACLs operates differently from a subnet mask. A wildcard mask is in essence the inverse of a subnet mask. With a subnet mask, the mask has ones (1's) in the bit positions that are used for the network address, and has zeros (0's) for the bit positions that are not used. In contrast, a wildcard mask has (0's) in a bit position that must be checked. A 1 in a bit position of the ACL mask indicates the corresponding bit can be ignored.

access-list

This command creates an IP *ACL* that is identified by the access list number, which is 1-99 for standard ACLs or 100-199 for extended ACLs. Table 14 on page 628 describes the parameters for the access-list command.

IP Standard ACL:

Format	`access-list 1-99 {remark comment} | {[sequence-number]} ] {deny | permit} {every | srcip srcmask | host srcip} [time-range time-range-name] [log] [assign-queue queue-id] [{mirror | redirect} unit/slot/port] [rate-limit rate burst-size]`
Mode	Global Config

IP Extended ACL:

Format	`access-list 100-199 {remark comment} | {[sequence-number]} [rule 1-1023] {deny | permit} {every | {{eigrp | gre | icmp | igmp | ip | ipinip | ospf | pim | tcp | udp | 0 -255} {srcip srcmask|any|host srcip}[range {portkey|startport} {portkey| endport} {eq|neq|lt|gt} {portkey|0-65535}{dstip dstmask|any| host dstip}[{range {portkey|startport} {portkey|endport} | {eq | neq | lt | gt} {portkey | 0-65535}] [flag [+fin | -fin] [+syn | -syn] [+rst | -rst] [+psh | -psh] [+ack | -ack] [+urg | -urg] [established]] [icmp-type icmp-type [icmp-code icmp-code] | icmp-message icmp-message] [igmp-type igmp-type] [fragments] [precedence precedence | tos tos [tosmask] | dscp dscp]}} [time-range time-range-name] [log] [assign-queue queue-id] [{mirror | redirect} unit/slot/port] [rate-limit rate burst-size]`
Mode	Global Config

Note

IPv4 extended ACLs have the following limitations for egress ACLs:

- Match on port ranges is not supported.
- The rate-limit command is not supported.

Table 14: ACL Command Parameters

Parameter	Description
remark *comment*	Use the remark keyword to add a comment (remark) to an IP standard or IP extended ACL. The remarks make the ACL easier to understand and scan. Each remark is limited to 100 characters. A remark can consist of characters in the range A-Z, a-z, 0-9, and special characters: space, hyphen, underscore. Remarks are displayed only in show running configuration. One remark per rule can be added for IP standard or IP extended ACL. User can remove only remarks that are not associated with a rule. Remarks associated with a rule are removed when the rule is removed
sequence-number	Specifies a sequence number for the ACL rule. Every rule receives a sequence number. A sequence number is specified by the user or is generated by the device. If a sequence number is not specified for the rule, a sequence number that is 10 greater than the last sequence number in the ACL is used and this rule is located in the end of the list. If this is the first ACL rule in the given ACL, a sequence number of 10 is assigned. If the calculated sequence number exceeds the maximum sequence number value, the ACL rule creation fails. It is not allowed to create a rule that duplicates an already existing one and a rule cannot be configured with a sequence number that is already used for another rule. For example, if user adds new ACL rule to ACL without specifying a sequence number, it is placed at the bottom of the list. By changing the sequence number, user can move the ACL rule to a different position in the ACL.
1-99 or *100-199*	Range 1 to 99 is the access list number for an IP standard ACL. Range 100 to 199 is the access list number for an IP extended ACL.
[rule *1-1023*]	Specifies the IP access list rule.
{deny | permit}	Specifies whether the IP ACL rule permits or denies an action. **Note:** Assign-queue, redirect, and mirror attributes are configurable for a deny rule, but they have no operational effect.
every	Match every packet.
{eigrp | gre | icmp | igmp | ip | ipinip | ospf | pim | tcp | udp | *0 -255*}	Specifies the protocol to filter for an extended IP ACL rule.
srcip srcmask|any|host *scrip*	Specifies a source IP address and source netmask for match condition of the IP ACL rule. Specifying any specifies *srcip* as 0.0.0.0 and *srcmask* as 255.255.255.255. Specifying host *A.B.C.D* specifies *srcip* as A.B.C.D and *srcmask* as 0.0.0.0.

Table 14: ACL Command Parameters (continued)

Parameter	Description
{{range{portkey|startport}{portkey|endport}|{eq|neq|lt|gt} {*portkey* | *0-65535*}]	This option is available only if the protocol is TCP or UDP. Specifies the source layer 4 port match condition for the IP ACL rule. You can use the port number, which ranges from 0-65535, or you specify the *portkey*, which can be one of the following keywords: • For TCP: *bgp*, *domain*, *echo*, *ftp*, *ftp-data*, *http*, *smtp*, *telnet*, *www*, *pop2*, *pop3*. • For UDP: *domain, echo, ntp, rip, snmp, tftp*, *time*, and *who*. For both TCP and UDP, each of these keywords translates into its equivalent port number, which is used as both the start and end of a port range. If *range* is specified, the IP ACL rule matches only if the layer 4 port number falls within the specified portrange. The *startport* and *endport* parameters identify the first and last ports that are part of the port range. They have values from 0 to 65535. The ending port must have a value equal or greater than the starting port. The starting port, ending port, and all ports in between will be part of the layer 4 port range. When *eq* is specified, the IP ACL rule matches only if the layer 4 port number is equal to the specified port number or portkey. When *lt* is specified, IP ACL rule matches if the layer 4 port number is less than the specified port number or portkey. It is equivalent to specifying the range as 0 to *specified port number* – 1. When *gt* is specified, the IP ACL rule matches if the layer 4 port number is greater than the specified port number or portkey. It is equivalent to specifying the range as *specified port number* + 1 to 65535. When *neq* is specified, IP ACL rule matches only if the layer 4 port number is not equal to the specified port number or portkey. Two rules are added in the hardware one with range equal to 0 to *specified port number* - 1 and one with range equal to *specified port number* + 1 to 65535 Port number matches only apply to unfragmented or first fragments.
dstip dstmask|any|host *dstip*	Specifies a destination IP address and netmask for match condition of the IP ACL rule. Specifying any implies specifying *dstip* as 0.0.0.0 and *dstmask* as 255.255.255.255. Specifying host A.B.C.D implies *dstip* as A.B.C.D and *dstmask* as 0.0.0.0.
[precedence *precedence* | tos *tos* [*tosmask*] | dscp *dscp*]	Specifies the TOS for an IP ACL rule depending on a match of precedence or DSCP values using the parameters *dscp*, *precedence*, *tos/tosmask*. *tosmask* is an optional parameter.

Table 14: ACL Command Parameters (continued)

Parameter	Description
flag [+fin | -fin] [+syn | -syn] [+rst | -rst] [+psh | -psh] [+ack | -ack] [+urg | -urg] [established]	This option is available only if the protocol is tcp. Specifies that the IP ACL rule matches on the TCP flags. When +*tcpflagname* is specified, a match occurs if the specified *tcpflagname* flag is set in the TCP header. When -*tcpflagname* is specified, a match occurs if the specified *tcpflagname* flag is *not* set in the TCP header. When established is specified, a match occurs if the specified RST or ACK bits are set in the TCP header. Two rules are installed in the hardware when the established option is specified.
[icmp-type *icmp-type* [icmp-code *icmp-code*] | icmp-message *icmp-message*]	This option is available only if the protocol is icmp. Specifies a match condition for *ICMP (Internet Control Message Protocol)* packets. When *icmp-type* is specified, the IP ACL rule matches on the specified ICMP message type, a number from 0 to 255. When *icmp-code* is specified, the IP ACL rule matches on the specified ICMP message code, a number from 0 to 255. Specifying *icmp-message* implies that both *icmp-type* and *icmp-code* are specified. The following icmp-messages are supported: *echo*, *echo-reply*, *host-redirect*, *mobile-redirect*, *net-redirect*, *net-unreachable*, *redirect*, *packet-too-big*, *port-unreachable*, *source-quench*, *router-solicitation*, *router-advertisement*, *time-exceeded*, *ttl-exceeded* and *unreachable*.
igmp-type igmp-type	This option is available only if the protocol is igmp. When igmp-type is specified, the IP ACL rule matches on the specified *IGMP (Internet Group Management Protocol)* message type, a number from 0 to 255.
fragments	Specifies that the IP ACL rule matches on fragmented IP packets.
[log]	Specifies that this rule is to be logged.
[time-range time-range-name]	Allows imposing time limitation on the ACL rule as defined by the parameter time-range-name. If a time range with the specified name does not exist and the ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied immediately. If a time range with specified name exists and the ACL containing this ACL rule is applied to an interface or bound to a VLAN, the ACL rule is applied when the time-range with specified name becomes active. The ACL rule is removed when the time-range with specified name becomes inactive. For information about configuring time ranges, see Time Range Commands for Time-Based ACLs on page 653.
[assign-queue *queue-id*]	Specifies the assign-queue, which is the queue identifier to which packets matching this rule are assigned.
[rate-limit *rate burst-size*]	Specifies the allowed rate of traffic as per the configured rate in kbps, and burst-size in kbytes.

no access-list

This command deletes an IP *ACL* that is identified by the parameter accesslistnumber from the system. The range for accesslistnumber 1-99 for standard access lists and 100-199 for extended access lists.

Format	no access-list *accesslistnumber* [rule *1-1023*]
Mode	Global Config

ip access-list

This command creates an extended IP *ACL* identified by name, consisting of classification fields defined for the IP header of an IPv4 frame. The name parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the IP access list. The rate-limit attribute configures the committed rate and the committed burst size.

If an IP ACL by this name already exists, this command enters IPv4-Access_List config mode to allow updating the existing IP ACL.

Note
The CLI mode changes to IPv4-Access-List Config mode when you successfully execute this command.

Format	ip access-list *name*
Mode	Global Config

no ip access-list

This command deletes the IP *ACL* identified by name from the system.

Format	no ip access-list *name*
Mode	Global Config

ip access-list rename

This command changes the name of an IP *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 newname already exists.

Format	ip access-list rename *name newname*
Mode	Global Config

ip access-list resequence

Use this command to renumber the sequence numbers of the entries for specified IP access list with the given increment value starting from a particular sequence number. The command is used to edit the

sequence numbers of *ACL* rules in the ACL and change the order in which entries are applied. This command is not saved in startup configuration and is not displayed in running configuration.

Note
If the generated sequence number exceeds the maximum sequence number, the ACL rule creation fails and an informational message is displayed.

Default	10
Format	`ip access-list resequence {name| id } starting-sequence-number increment`
Mode	Global Config

Parameter	Description
starting-sequence-number	The sequence number from which to start. The range is 1–2147483647. The default is 10.
increment	The amount to increment. The range is 1–2147483647. The default is 10.

{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.

Format	`[sequence-number] {deny | permit} {every | {{eigrp | gre | icmp | igmp | ip | ipinip | ospf | pim | tcp | udp | 0 -255} {srcip srcmask | any | host srcip} [{range {portkey | startport} {portkey | endport} | {eq | neq | lt | gt} {portkey | 0-65535}] {dstip dstmask | any | host dstip} [{range {portkey | startport} {portkey | endport} | {eq | neq | lt | gt} {portkey | 0-65535}] [flag [+fin | -fin] [+syn | -syn] [+rst | -rst] [+psh | -psh] [+ack | -ack] [+urg | -urg] [established]] [icmp-type icmp-type [icmp-code icmp-code] | icmp-message icmp-message] [igmp-type igmp-type] [fragments] [precedence precedence | tos tos [tosmask] | dscp dscp]| [ttl eq 0-255]}} [time-range time-range-name] [log] [assign-queue queue-id] [rate-limit rate burst-size]`
Mode	Ipv4-Access-List Config

Note
An implicit deny all IP rule always terminates the access list.

Note

For IPv4, the following are not supported for egress ACLs:

- A match on port ranges.
- The rate-limit command.

The time-range parameter allows imposing time limitation on the IP ACL rule as defined by the specified time range. If a time range with the specified name does not exist and the ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied immediately. If a time range with specified name exists and the ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied when the time-range with specified name becomes active. The ACL rule is removed when the time-range with specified name becomes inactive. For information about configuring time ranges, see Time Range Commands for Time-Based ACLs on page 653.

The assign-queue parameter allows specification of a particular hardware queue for handling traffic that matches this rule. The allowed queue-id value is 0-(n-1), where n is the number of user configurable queues available for the hardware platform. The assign-queue parameter is valid only for a permit rule.

The permit command's optional attribute rate-limit allows you to permit only the allowed rate of traffic as per the configured rate in kbps, and burst-size in kbytes.

Parameter	Description
sequence-number	The sequence-number specifies the sequence number for the ACL rule. The sequence number is specified by the user or is generated by device. If a sequence number is not specified for the rule, a sequence number that is 10 greater than the last sequence number in ACL is used and this rule is placed at the end of the list. If this is the first ACL rule in the given ACL, a sequence number of 10 is assigned. If the calculated sequence number exceeds the maximum sequence number value, the ACL rule creation fails. A rule cannot be created that duplicates an already existing one and a rule cannot be configured with a sequence number that is already used for another rule. For example, if user adds new ACL rule to ACL without specifying a sequence number, it is placed at the bottom of the list. By changing the sequence number, the user can move the ACL rule to a different position in the ACL.
{deny | permit}	Specifies whether the IP ACL rule permits or denies the matching traffic.
every	Match every packet.
{eigrp | gre | icmp | igmp | ip | ipinip | ospf | pim | tcp | udp | 0 -255}	Specifies the protocol to match for the IP ACL rule.
srcip srcmask | any | host *srcip*	Specifies a source IP address and source netmask to match for the IP ACL rule. Specifying "any" implies specifying srcip as "0.0.0.0" and srcmask as "255.255.255.255". Specifying "host A.B.C.D" implies srcip as "A.B.C.D" and srcmask as "0.0.0.0".

Parameter	Description
[{range {*portkey* | *startport*} {*portkey* | *endport*} | {eq | neq | lt | gt} {*portkey* | *0-65535*}]	This option is available only if the protocol is tcp or udp. Specifies the layer 4 port match condition for the IP ACL rule. Port number can be used, which ranges from 0-65535, or the portkey, which can be one of the following keywords: • For tcp protocol: bgp, domain, echo, ftp, ftp-data, http, smtp, telnet, www, pop2, pop3 • For udp protocol: domain, echo, ntp, rip, snmp, tftp, time, who Each of these keywords translates into its equivalent port number. When range is specified, the IP ACL rule matches only if the layer 4 port number falls within the specified port range. The startport and endport parameters identify the first and last ports that are part of the port range. They have values from 0 to 65535. The ending port must have a value equal to or greater than the starting port. The starting port, ending port, and all ports in between will be part of the layer 4 port range. When eq is specified, IP ACL rule matches only if the layer 4 port number is equal to the specified port number or portkey. When lt is specified, IP ACL rule matches if the layer 4 port number is less than the specified port number or portkey. It is equivalent to specifying the range as 0 to *specified port number* – 1. When gt is specified, IP ACL rule matches if the layer 4 port number is greater than the specified port number or portkey. It is equivalent to specifying the range as *specified port number* + 1 to 65535. When neq is specified, IP ACL rule matches only if the layer 4 port number is not equal to the specified port number or port key. Two rules are added in the hardware one with range equal to 0 to *specified port number* - 1 and one with range equal to *specified port number* + 1 to 65535. Port number matches only apply to unfragmented or first fragments.
dstip dstmask | any | host *dstip*	Specifies a destination IP address and netmask for match condition of the IP ACL rule. Specifying any implies specifying dstip as 0.0.0.0 and dstmask as 255.255.255.255. Specifying host A.B.C.D implies dstip as A.B.C.D and dstmask as 0.0.0.0.

Parameter	Description
[precedence *precedence* | tos *tos* [*tosmask*] | dscp *dscp*]	Specifies the TOS for an IP ACL rule depending on a match of precedence or DSCP values using the parameters dscp, precedence, tos/tosmask. tosmask is an optional parameter.
flag [+fin | -fin] [+syn | -syn] [+rst | -rst] [+psh | -psh] [+ack | -ack] [+urg | -urg] [established]	Specifies that the IP ACL rule matches on the tcp flags. When +*tcpflagname* is specified, a match occurs if the specified *tcpflagname* flag is set in the TCP header. When -*tcpflagname* is specified, a match occurs if the specified *tcpflagname* flag is NOT set in the TCP header. When established is specified, a match occurs if either the specified RST or ACK bits are set in the TCP header. Two rules are installed in hardware to when the established option is specified. This option is available only if protocol is tcp.
[icmp-type *icmp-type* [icmp-code *icmp-code*] | icmp-message *icmp-message*]	This option is available only if the protocol is *ICMP*. Specifies a match condition for ICMP packets. When icmp-type is specified, IP ACL rule matches on the specified ICMP message type, a number from 0 to 255. When icmp-code is specified, IP ACL rule matches on the specified ICMP message code, a number from 0 to 255. Specifying icmp-message implies both icmp-type and icmp-code are specified. The following icmp-messages are supported: echo, echo-reply, host-redirect, mobile-redirect, net-redirect, net-unreachable, redirect, packet-too-big, port-unreachable, source-quench, router-solicitation, router-advertisement, time-exceeded, ttl-exceeded and unreachable. The ICMP message is decoded into corresponding ICMP type and ICMP code within that ICMP type.
igmp-type igmp-type	This option is visible only if the protocol is *IGMP*. When igmp-type is specified, the IP ACL rule matches on the specified IGMP message type, a number from 0 to 255.
fragments	Specifies that IP ACL rule matches on fragmented IP packets.
ttl eq	Specifies that the IP ACL rule matches on packets with the specified Time To Live (TTL) value.
log	Specifies that this rule is to be logged.
time-range *time-range-name*	Allows imposing a time limitation on the ACL rule as defined by the parameter time-range-name. If a time range with the specified name does not exist and the ACL containing this ACL rule is applied to an interface or bound to a VLAN, the ACL rule is applied immediately. If a time range with specified name exists and the ACL containing this ACL rule is applied to an interface or bound to a VLAN, the ACL rule is applied when the time-range with specified name becomes active. The ACL rule is removed when the time-range with specified name becomes inactive.
assign-queue queue-id	Specifies the assign-queue, which is the queue identifier to which packets matching this rule are assigned.
rate-limit rate burst-size	Specifies the allowed rate of traffic as per the configured rate in kbps, and burst-size in kbytes.

The following shows an example of the command.

```
(Extreme 220) (Config) (Config)#ip access-list ip1
(Extreme 220) (Config-ipv4-acl)#permit icmp any any rate-limit 32 16
(Extreme 220) (Config-ipv4-acl)#exit
```

no sequence-number

Use this command to remove the *ACL* rule with the specified sequence number from the ACL.

Format	`no sequence-number`
Mode	Ipv4-Access-List Config

ip access-group

This command either attaches a specific IP *ACL* identified by accesslistnumber or name to an interface (including VLAN routing interfaces), range of interfaces, or all interfaces; or associates it with a VLAN ID in a given direction. The parameter name is the name of the Access Control List.

An optional sequence number may be specified to indicate the order of this IP access list relative to other IP access lists already assigned to this interface and direction. A lower number indicates higher precedence order. If a sequence number is already in use for this interface and direction, the specified access list replaces the currently attached IP access list using that sequence number. If the sequence number is not specified for this command, a sequence number that is one greater than the highest sequence number currently in use for this interface and direction is used.

An optional control-plane is specified to apply the ACL on CPU port. The IPv4 control packets like RADIUS and TACACS+ are also dropped because of the implicit deny all rule added at the end of the list. To overcome this, permit rules must be added to allow the IPv4 control packets.

Note
The keyword control-plane is only available in Global Config mode.

Note
You should be aware that the out option may or may not be available, depending on the platform.

Default	none
Format	`ip access-group {accesslistnumber|name} {{control-plane|in|out}|vlan vlan-id {in|out}} [sequence 1-4294967295]`
Modes	• Interface Config • Global Config

Parameter	Description
accesslistnumber	Identifies a specific IP ACL. The range is 1 to 199.
sequence	A optional sequence number that indicates the order of this IP access list relative to the other IP access lists already assigned to this interface and direction. The range is 1 to 4294967295.
vlan-id	A VLAN ID associated with a specific IP ACL in a given direction.
name	The name of the Access Control List.

The following shows an example of the command.

```
(Extreme 220) (Config) #ip access-group ip1 control-plane
```

no ip access-group

This command removes a specified IP *ACL* from an interface.

Default	none
Format	`no ip access-group {accesslistnumber|name} {{control-plane|in|out}|vlan vlan-id {in|out}}`
Mode	• Interface Config • Global Config

The following shows an example of the command.

```
(Extreme 220) (Routing)(Config)#no ip access-group ip1 control-plane
```

acl-trapflags

This command enables the *ACL* trap mode.

Default	Disabled
Format	`acl-trapflags`
Mode	Global Config

no acl-trapflags

This command disables the *ACL* trap mode.

Format	`no acl-trapflags`
Mode	Global Config

show ip access-lists

Use this command to view summary information about all IP *ACL*s 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. It displays committed rate, committed burst size, and ACL rule hit count of packets matching the configured ACL rule within an ACL. This counter value rolls-over on reaching the maximum value. There is a dedicated counter for each ACL rule. ACL counters do not interact with PBR counters.

For ACL with multiple rules, once a match occurs at any one specific rule, counters associated with this rule only get incremented for example, consider an ACL with three rules, after matching rule two, counters for rule three would not be incremented).

For ACL counters, if an ACL rule is configured without RATE-LIMIT, the counter value is count of forwarded/discarded packets (for example: If burst of 100 packets sent from IXIA, the Counter value is 100).

If an ACL rule is configured with RATE LIMIT, the counter value will be the MATCHED packet count. If the sent traffic rate exceeds the configured limit, counters will still display matched packet count (despite getting dropped beyond the configured limit since match criteria is met) that would equal the sent rate. For example, if rate limit is set to 10 kbps and 'matching' traffic is sent at 100 kbps, counters would reflect 100 kbps value. If the sent traffic rate is less than the configured limit, counters would display only matched packet count. Either way, only matched packet count is reflected in the counters, irrespective of whether they get dropped or forwarded. ACL counters do not interact with diffserv policies.

Format	`show ip access-lists [accesslistnumber | name]`
Mode	Privileged EXEC

Column	Meaning
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:

Note
Only the access list fields that you configure are displayed. Thus, the command output varies based on the match criteria configured within the rules of an ACL.

Column	Meaning
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	Whether this access list applies to every packet. Possible values are True or False.
Protocol	The protocol to filter for this rule.

Column	Meaning
ICMP Type	This is shown only if the protocol is *ICMP*. The ICMP message type for this rule.
Starting Source L4 port	The starting source layer 4 port.
Ending Source L4 port	The ending source layer 4 port.
Starting Destination L4 port	The starting destination layer 4 port.
Ending Destination L4 port	The ending destination layer 4 port.
ICMP Code	This is shown only if the protocol is ICMP. The ICMP message code for this rule.
Fragments	If the ACL rule matches on fragmented IP packets.
Committed Rate	The committed rate defined by the rate-limit attribute.
Committed Burst Size	The committed burst size defined by the rate-limit attribute.
Source IP Address	The source IP address for this rule.
Source IP Mask	The source IP Mask for this rule.
Source L4 Port Keyword	The source port for this rule.
Destination IP Address	The destination IP address for this rule.
Destination IP Mask	The destination IP Mask for this rule.
Destination L4 Port Keyword	The destination port for this rule.
IP DSCP	The value specified for IP DSCP.
IP Precedence	The value specified IP Precedence.
IP TOS	The value specified for IP TOS.
Fragments	Specifies whether the IP ACL rule matches on fragmented IP packets is enabled.
TTL Field Value	The value specified for the TTL.
Log	Displays when you enable logging for the rule.
Assign Queue	The queue identifier to which packets matching this rule are assigned.
Mirror Interface	The unit/slot/port to which packets matching this rule are copied.
Redirect Interface	The unit/slot/port to which packets matching this rule are forwarded.
Time Range Name	Displays the name of the time-range if the IP ACL rule has referenced a time range.
Rule Status	Status (Active/Inactive) of the IP ACL rule.
ACL Hit Count	The ACL rule hit count of packets matching the configured ACL rule within an ACL.
ACL Hit Count	The ACL rule hit count of packets matching the configured ACL rule within an ACL. This counter value rolls-over on reaching the maximum value. There is a dedicated counter for each ACL rule. ACL counters do not interact with PBR counters. For ACL with multiple rules, once a match occurs at any one specific rule, counters associated with this rule only get incremented, (for example

Column	Meaning
	consider an ACL with three rules, after matching rule 2, counters for rule 3 would not be incremented). For ACL counters, if an ACL rule is configured without RATE-LIMIT, the counter value is count of forwarded/discarded packets. (Example: If burst of 100 packets sent from IXIA, Counter value is 100). And if ACL rule is configured with RATE LIMIT, the counter value will be the MATCHED packet count. If the sent traffic rate exceeds the configured limit, counters would still display matched packet count (despite getting dropped beyond the configured limit since match criteria is met) which would equal the sent rate. For example, if rate limit is set to 10 kbps and 'matching' traffic is sent at 100 kbps, counters would reflect 100 kbps value. If the sent traffic rate is less than the configured limit, counters display only matched packet count. Either way, only matched packet count is reflected in the counters, irrespective of whether they get dropped or forwarded. ACL counters do not interact with diffserv policies.

The following example shows CLI display output for the command.

```
(Extreme 220) (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
```

show access-lists

This command displays IP ACLs, IPv6 *ACL*s, and MAC access control lists information for a designated interface and direction. 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. Use the **control-plane** keyword to display the ACLs applied on the CPU port.

Format	`show access-lists interface {`*`unit/slot/port`* `in | out | control-plane}`
Mode	Privileged EXEC

Column	Meaning
ACL Type	Type of access list (IP, IPv6, or MAC).

Column	Meaning
ACL ID	Access List name for a MAC or IPv6 access list or the numeric identifier for an IP access list.
Sequence Number	An optional sequence number may be specified to indicate the order of this access list relative to other access lists already assigned to this interface and direction. A lower number indicates higher precedence order. If a sequence number is already in use for this interface and direction, the specified access list replaces the currently attached access list using that sequence number. If the sequence number is not specified by the user, a sequence number that is one greater than the highest sequence number currently in use for this interface and direction is used. Valid range is (1 to 4294967295).
in|out	• in – Display Access List information for a particular interface and the in direction. • out – Display Access List information for a particular interface and the out direction.

The following shows an example of the command.

```
(Extreme 220) (Routing) #show access-lists interface control-plane
ACL Type             ACL ID                    Sequence Number
--------          -------------------------------  ---------------
IPv6             ip61                                  1
```

show access-lists vlan

This command displays Access List information for a particular VLAN ID. The vlan-id parameter is the VLAN ID of the VLAN with the information to view. The {in | out} options specifies the direction of the VLAN *ACL* information to view.

Format	`show access-lists vlan` *`vlan-id`* `in|out`
Mode	Privileged EXEC

Column	Meaning
ACL Type	Type of access list (IP, IPv6, or MAC).
ACL ID	Access List name for a MAC or IPv6 access list or the numeric identifier for an IP access list.
Sequence Number	An optional sequence number may be specified to indicate the order of this access list relative to other access lists already assigned to this interface and direction. A lower number indicates higher precedence order. If a sequence number is already in use for this interface and direction, the specified access list replaces the currently attached access list using that sequence number. If the sequence number is not specified by the user, a sequence number that is one greater than the highest sequence number currently in use for this interface and direction is used. Valid range is (1 to 4294967295).

IPv6 Access Control List Commands

This section describes the commands used to configure IPv6 *ACL* settings. IPv6 ACLs ensure that only authorized users have access to specific resources and block any unwarranted attempts to reach network resources.

The following rules apply to IPv6 ACLs:

- The maximum number of ACLs you create is 100, regardless of type.
- The system supports only Ethernet II frame types.

- The maximum number of rules per IPv6 ACL is hardware dependent.

ipv6 access-list

This command creates an IPv6 *ACL* identified by name, consisting of classification fields defined for the IP header of an IPv6 frame. The name parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the IPv6 access list. The rate-limit attribute configures the committed rate and the committed burst size.

If an IPv6 ACL by this name already exists, this command enters IPv6-Access-List config mode to allow updating the existing IPv6 ACL.

Note
The CLI mode changes to IPv6-Access-List Config mode when you successfully execute this command.

Format	`ipv6 access-list` *name*
Mode	Global Config

no ipv6 access-list

This command deletes the IPv6 *ACL* identified by name from the system.

Format	`no ipv6 access-list` *name*
Mode	Global Config

ipv6 access-list rename

This command changes the name of an IPv6 *ACL*. The name parameter is the name of an existing IPv6 ACL. The newname parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the IPv6 access list.

This command fails is an IPv6 ACL by the name newname already exists.

Format	`ipv6 access-list rename` *name newname*
Mode	Global Config

ipv6 access-list resequence

Use this command to renumber the sequence numbers of the entries for specified IPv6 access list with the given increment value starting from a particular sequence number. The command is used to edit the

sequence numbers of *ACL* rules in the ACL and change the order in which entries are applied. This command is not saved in startup configuration and is not displayed in running configuration.

Note
If the generated sequence number exceeds the maximum sequence number, the ACL rule creation fails and an informational message is displayed.

Default	10
Format	`ipv6 access-list resequence {name| id } starting-sequence-number increment`
Mode	Global Config

Parameter	Description
starting-sequence-number	The sequence number from which to start. The range is 1–2147483647. The default is 10.
increment	The amount to increment. The range is 1–2147483647. The default is 10.

{deny | permit} (IPv6)

This command creates a new rule for the current IPv6 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 IPv6 address fields may be specified using the keyword any to indicate a match on any value in that field. The remaining command parameters are all optional, but the most frequently used parameters appear in the same relative order as shown in the command format.

Format	`{deny | permit} {every | {{icmpv6 | ipv6 | tcp | udp | 0-255} {source-ipv6-prefix/prefix-length | any | host source-ipv6-address} [{range {portkey | startport} {portkey | endport} | {eq | neq | lt | gt} {portkey | 0-65535}] {destination-ipv6-prefix/prefix-length | any | host destination-ipv6-address} [{range {portkey | startport} {portkey | endport} | {eq | neq | lt | gt} {portkey | 0-65535}] [flag [+fin | -fin] [+syn | -syn] [+rst | -rst] [+psh | -psh] [+ack | -ack] [+urg | -urg] [established]] [flow-label value] [icmp-type icmp-type [icmp-code icmp-code] | icmp-message icmp-message] [routing] [fragments] [sequence sequence-number] [dscp dscp]}} [log] [assign-queue queue-id] [rate-limit rate burst-size]`
Mode	IPv6-Access-List Config

Note
An implicit deny all IPv6 rule always terminates the access list.

The time-range parameter allows imposing time limitation on the IPv6 ACL rule as defined by the parameter time-range-name. If a time range with the specified name does not exist and the IPv6 ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied

immediately. If a time range with specified name exists and the IPv6 ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied when the time-range with specified name becomes active. The ACL rule is removed when the time-range with specified name becomes inactive. For information about configuring time ranges, see Time Range Commands for Time-Based ACLs on page 653.

The assign-queue parameter allows specification of a particular hardware queue for handling traffic that matches this rule. The allowed queue-id value is 0-(n-1), where n is the number of user configurable queues available for the hardware platform. The assign-queue parameter is valid only for a permit rule.

The permit command's optional attribute rate-limit allows you to permit only the allowed rate of traffic as per the configured rate in kbps, and burst-size in kbytes.

IPv6 ACLs have the following limitations:

- Port ranges are not supported for egress IPv6 ACLs.
- The IPv6 ACL fragment keyword matches only on the first IPv6 extension header (next header code 44). If the fragment header appears in the second or subsequent header, it is not matched.
- The IPv6 ACL routing keyword matches only on the first IPv6 extension header (next header code 43). If the fragment header appears in the second or subsequent header, it is not matched.
- The rate-limit command is not supported for egress IPv6 ACLs.

Parameter	Description
{deny | permit}	Specifies whether the IPv6 ACL rule permits or denies the matching traffic.
Every	Specifies to match every packet.
{*protocolkey* | *number*}	Specifies the protocol to match for the IPv6 ACL rule. The current list is: *icmpv6*, *ipv6*, *tcp*, and *udp*.
source-ipv6-prefix/prefix-length | any | host source-ipv6-address	Specifies a source IPv6 source address and prefix length to match for the IPv6 ACL rule. Specifying any implies specifying "::/0 " Specifying *host source-ipv6-address* implies matching the specified IPv6 address. This *source-ipv6-address* argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.

Parameter	Description
[{range {*portkey* | *startport*} {*portkey* | *endport*} | {eq | neq | lt | gt} {*portkey* | *0–65535*}]	This option is available only if the protocol is TCP or UDP. Specifies the layer 4 port match condition for the IPv6 ACL rule. A port number can be used, in the range 0-65535, or the portkey, which can be one of the following keywords: • For TCP: *bgp*, *domain*, *echo*, *ftp*, *ftp-data*, *http*, *smtp*, *telnet*, *www*, *pop2*, *pop3* • For UDP: *domain*, *echo*, *ntp*, *rip*, *snmp*, *tftp*, *time*, *who*. Each of these keywords translates into its equivalent port number. When range is specified, IPv6 ACL rule matches only if the layer 4 port number falls within the specified portrange. The startport and endport parameters identify the first and last ports that are part of the port range. They have values from 0 to 65535. The ending port must have a value equal or greater than the starting port. The starting port, ending port, and all ports in between are part of the layer 4 port range. When eq is specified, IPv6 ACL rule matches only if the layer 4 port number is equal to the specified port number or portkey. When lt is specified, IPv6 ACL rule matches if the layer 4 port number is less than the specified port number or portkey. It is equivalent to specifying the range as 0 to *specified port number* - 1. When gt is specified, IPv6 ACL rule matches if the layer 4 port number is greater than the specified port number or portkey. It is equivalent to specifying the range as *specified port number* + 1 to 65535. When neq is specified, IPv6 ACL rule matches only if the layer 4 port number is not equal to the specified port number or portkey. Two rules are added in the hardware one with range equal to 0 to *specified port number* - 1 and one with range equal to *specified port number* + 1 to 65535.
destination-ipv6-prefix/prefix-length | any | host destination-ipv6-address	Specifies a destination IPv6 source address and prefix length to match for the IPv6 ACL rule. Specifying any implies specifying "::/0 " Specifying *host* destination-ipv6-address implies matching the specified IPv6 address. This *destination*-ipv6-address argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.

Parameter	Description
sequence *sequence-number*	Specifies a sequence number for the ACL rule. Every rule receives a sequence number. The sequence number is specified by the user or is generated by the device. If a sequence number is not specified for the rule, a sequence number that is 10 greater than the last sequence number in ACL is used and this rule is placed at the end of the list. If this is the first ACL rule in the given ACL, a sequence number of 10 is assigned. If the calculated sequence number exceeds the maximum sequence number value, the ACL rule creation fails. It is not allowed to create a rule that duplicates an already existing one. A rule cannot be configured with a sequence number that is already used for another rule. For example, if a user adds new ACL rule to ACL without specifying a sequence number, it is placed at the bottom of the list. By changing the sequence number, user can move the ACL rule to a different position in the ACL
[dscp dscp]	Specifies the dscp value to match for the IPv6 rule.
flag [+fin | -fin] [+syn | -syn] [+rst | -rst] [+psh | -psh] [+ack | -ack] [+urg | -urg] [established]	Specifies that the IPv6 ACL rule matches on the tcp flags. When +*tcpflagname* is specified, a match occurs if the specified *tcpflagname* flag is set in the TCP header. When -*tcpflagname* is specified, a match occurs if the specified *tcpflagname* flag is NOT set in the TCP header. When established is specified, a match occurs if the specified either RST or ACK bits are set in the TCP header. Two rules are installed in hardware to when “established” option is specified. This option is visible only if protocol is “tcp”.

Parameter	Description
[icmp-type *icmp-type* [icmp-code *icmp-code*] | icmp-message *icmp-message*]	This option is available only if the protocol is icmpv6. Specifies a match condition for *ICMP* packets. When icmp-type is specified, IPv6 ACL rule matches on the specified ICMP message type, a number from 0 to 255. When icmp-code is specified, IPv6 ACL rule matches on the specified ICMP message code, a number from 0 to 255. Specifying icmp-message implies both icmp-type and icmp-code are specified. The following icmp-messages are supported: *destination-unreachable*, *echo-reply*, *echo-request*, *header*, *hop-limit*, *mld-query*, *mld-reduction*, *mld-report*, *nd-na*, *nd-ns*, *next-header*, *no-admin*, *no-route*, *packet-too-big*, *port-unreachable*, *router-solicitation*, *router-advertisement*, *router-renumbering*, *time-exceeded*, and *unreachable*. The ICMP message is decoded into the corresponding ICMP type and ICMP code within that ICMP type.
Fragments	Specifies that IPv6 ACL rule matches on fragmented IPv6 packets (Packets that have the next header field is set to 44).
Routing	Specifies that IPv6 ACL rule matches on IPv6 packets that have routing extension headers (the next header field is set to 43).
Log	Specifies that this rule is to be logged.
time-range time-range-name	Allows imposing a time limitation on the ACL rule as defined by the parameter *time-range-name*. If a time range with the specified name does not exist and the ACL containing this ACL rule is applied to an interface or bound to a VLAN, the ACL rule is applied immediately. If a time range with the specified name exists and the ACL containing this ACL rule is applied to an interface or bound to a VLAN, the ACL rule is applied when the time-range with the specified name becomes active. The ACL rule is removed when the time-range with specified name becomes inactive.
assign-queue queue-id	Specifies the assign-queue, which is the queue identifier to which packets matching this rule are assigned.
rate-limit rate burst-size	Specifies the allowed rate of traffic as per the configured rate in kbps, and burst-size in kbytes.

The following shows an example of the command.

```
(Extreme 220) (Config) #ipv6 access-list ip61
(Extreme 220) (Config-ipv6-acl)#permit udp any any rate-limit 32 16
(Extreme 220) (Config-ipv6-acl)#exit
```

no sequence-number

Use this command to remove the *ACL* rule with the specified sequence number from the ACL.

Format	`no sequence-number`
Mode	Ipv6-Access-List Config

ipv6 traffic-filter

This command either attaches a specific IPv6 *ACL* identified by name to an interface or range of interfaces, or associates it with a VLAN ID in a given direction. The name parameter must be the name of an existing IPv6 ACL.

An optional sequence number may be specified to indicate the order of this mac access list relative to other IPv6 access lists already assigned to this interface and direction. A lower number indicates higher precedence order. If a sequence number is already in use for this interface and direction, the specifiedIPv6 access list replaces the currently attached IPv6 access list using that sequence number. If the sequence number is not specified for this command, a sequence number that is one greater than the highest sequence number currently in use for this interface and direction is used.

This command specified in Interface Config mode only affects a single interface, whereas the Global Config mode setting is applied to all interfaces. The **`vlan`** keyword is only valid in the Global Config mode. 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 ACL on CPU port. The IPv6 control packets like IGMPv6 are also dropped because of the implicit deny all rule added at the end of the list. To overcome this, permit rules must be added to allow the IPv6 control packets.

Note
The keyword control-plane is only available in Global Config mode.

Note
You should be aware that the *out* option may or may not be available, depending on the platform.

Format	`ipv6 traffic-filter name {{control-plane |in|out}|vlan vlan-id {in|out}} [sequence 1-4294967295]`
Modes	• Global Config • Interface Config

The following shows an example of the command.

```
(Extreme 220) (Routing)(Config)#ipv6 traffic-filter ip61 control-plane
```

no ipv6 traffic-filter

This command removes an IPv6 *ACL* identified by name from the interface(s) in a given direction.

Format	`no ipv6 traffic-filter [name {control-plane | in | out} | vlan`*`vlan-id`* `in | out}]`
Modes	• Global Config • Interface Config

The following shows an example of the command.

```
(Extreme 220) (Config) #no ipv6 traffic-filter ip61 control-plane
```

show ipv6 access-lists

This command displays summary information of all the IPv6 Access lists. Use the access list name to display detailed information of a specific IPv6 *ACL*.

This command displays information about the attributes icmp-type, icmp-code, fragments, routing, tcp flags, and source and destination L4 port ranges. It displays committed rate, committed burst size, and ACL rule hit count of packets matching the configured ACL rule within an ACL. This counter value rolls-over on reaching the maximum value. There is a dedicated counter for each ACL rule. ACL counters do not interact with PBR counters.

For ACL with multiple rules, once a match occurs at any one specific rule, counters associated with this rule only get incremented (for example, consider an ACL with three rules, after matching rule two, counters for rule three would not be incremented).

For ACL counters, If an ACL rule is configured without RATE-LIMIT, the counter value is a count of the forwarded/discarded packets. (For example: for a burst of 100 packets, the Counter value is 100).

If an ACL rule is configured with RATE LIMIT, the counter value is that of the MATCHED packet count. If the sent traffic rate exceeds the configured limit, the counters still display matched packet count (despite getting dropped beyond the configured limit since match criteria is met) that equals the sent rate. For example, if the rate limit is set to 10 kbps and ‘matching’ traffic is sent at 100 kbps, counters would reflect 100 kbps value. If the sent traffic rate is less than the configured limit, the counters display only the matched packet count. Either way, only the matched packet count is reflected in the counters, irrespective of whether they get dropped or forwarded. ACL counters do not interact with diffserv policies.

Format	`show ipv6 access-lists [name]`
Mode	Privileged EXEC

Note
Only the access list fields that you configure are displayed. Thus, the command output varies based on the match criteria configured within the rules of an ACL.

Column	Meaning
Rule Number	The ordered rule number identifier defined within the IPv6 ACL.
Action	The action associated with each rule. The possible values are Permit or Deny.
Match All	Whether this access list applies to every packet. Possible values are True or False.

Column	Meaning
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.
Log	Displays when you enable logging for the rule.
Assign Queue	The queue identifier to which packets matching this rule are assigned.
Mirror Interface	The *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.
Rule Status	Status (Active/Inactive) of the IPv6 ACL rule.
ACL Hit Count	The ACL rule hit count of packets matching the configured ACL rule within an ACL.

The following example shows CLI display output for the command.

```
(Extreme 220) (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
ACL hit count .............................0
```

Management Access Control and Administration List

In order to ensure the security of the switch management features, the administrator may elect to configure a management access control list. The Management Access Control and Administration List (MACAL) feature is used to ensure that only known and trusted devices are allowed to remotely manage the switch via TCP/IP.

MACALs can be applied only to in-band ports and cannot be applied to the service port.

management access-list

Use this command to create a management access list and to enter access-list configuration mode, where you must define the denied or permitted access conditions with the deny and `permit` commands. If no match criteria are defined, the default is deny. If you reenter to an access- list context,

the new rules would be entered at the end of the access-list. Use the `management access-class` command to choose the active access-list. The active management list cannot be updated or removed. The name value can be up to 32 characters.

Format	`management access-list` *name*
Mode	Global Config

no management access-list

This command deletes the MACAL identified by name from the system.

Format	`no management access-list` *name*
Mode	Global Config

{deny | permit} (Management ACAL)

This command creates a new rule for the current management access list. A rule may either deny or permit traffic according to the specified classification fields. Rules with ethernet, vlan and port-channel parameters will be valid only if an IP address is defined on the appropriate interface. Each rule should have a unique priority.

Format	*{deny | permit} [ethernet interface-number | vlan vlan-id | port-channel number] [service service] [priority priority-value]* *{deny | permit} ip-source ip-address [mask mask | prefix-length] [ethernet interface-number | vlan vlan-id | port-channel number] [service service] [priority priority-value]*
Mode	Management-ACAL Config

Parameter	Description
ethernet	Ethernet port number.
ip-source	Source IP address
port-channel	Port-channel number.
priority	Priority for rule.
service	Service type condition, which can be one of the following key words: • java • tftp • telnet • ssh • http • https • snmp • sntp • any
vlan	VLAN number.

Parameter	Description
mask	The network mask of the source IP address (0–32)
prefix-length	The number of bits that comprise the source IP address prefix. prefix length must be preceded by a forward slash (/).

The following example shows how to configure two management interfaces:

```
ethernet 0/1 and ethernet 0/9.
(Extreme 220) (Config) #management access-list mlist
(Extreme 220) (config-macal)#permit ethernet 0/1 priority 63
(Extreme 220) (config-macal)#permit ethernet 0/9 priority 64
(Extreme 220) (config-macal)#exit
(Extreme 220) (Config) #management access-class mlist
```

The following example shows how to configure all the interfaces to be management interfaces except for two interfaces: ethernet 0/1 and ethernet 0/9.

```
(Extreme 220) (Config) #management access-list mlist
(Extreme 220) (config-macal)#deny ethernet 0/1 priority 62
(Extreme 220) (config-macal)#deny ethernet 0/9 priority 63
(Extreme 220) (config-macal)#permit priority 64
(Extreme 220) (config-macal)#exit
```

management access-class

Use this command to restrict management connections. The **`console-only`** keyword specifies that the device can be managed only from the console.

Format	`management access-class {console-only | name}`
Mode	Global Config

no management access-class

This command disables the management restrictions

Format	`no management access-class`
Mode	Global Config

show management access-list

This command displays management access-lists.

Format	`show management access-list [name]`
Mode	Privileged EXEC

The following example shows CLI display output for the command.

```
(Extreme 220) (Routing) # show management access-list
List Name..................................... mlist
```

```
List Admin Mode.............................. Disabled
Packets Filtered............................. 0
Rules:
permit ethernet 0/1 priority 63
permit ethernet 0/9 priority 64
NOTE: All other access is implicitly denied.
```

show management access-class

This command displays information about the active management access list.

Format	`show management access-class [name]`
Mode	Privileged EXEC

The following example shows CLI display output for the command.

```
(Extreme 220) (Routing) #show management access-class
Management access-class is enabled, using access list mlist
```

Time Range Commands for Time-Based ACLs

Time-based *ACL*s allow one or more rules within an ACL to be based on time. Each ACL rule within an ACL except for the implicit deny all rule can be configured to be active and operational only during a specific time period. The time range commands allow you to define specific times of the day and week in order to implement time-based ACLs. The time range is identified by a name and can then be referenced by an ACL rule defined with in an ACL.

time-range

Use this command to create a time range identified by name, consisting of one absolute time entry and/or one or more periodic time entries. The name parameter is a case-sensitive, alphanumeric string from 1 to 31 characters that uniquely identifies the time range. An alpha-numeric string is defined as consisting of only alphabetic, numeric, dash, underscore, or space characters.

If a time range by this name already exists, this command enters Time-Range config mode to allow updating the time range entries

Note
When you successfully execute this command, the CLI mode changes to Time-Range Config mode.

Format	`time-range name`
Mode	Global Config

no time-range

This command deletes a time-range identified by name.

Format	`no time-range` *`name`*
Mode	Global Config

absolute

Use this command to add an absolute time entry to a time range. Only one absolute time entry is allowed per time-range. The time parameter is based on the currently configured time zone.

The [start time date] parameters indicate the time and date at which the configuration that referenced the time range starts going into effect. The time is expressed in a 24-hour clock, in the form of hours:minutes. For example, 8:00 is 8:00 am and 20:00 is 8:00 pm. The date is expressed in the format day month year. If no start time and date are specified, the configuration statement is in effect immediately.

The [end time date] parameters indicate the time and date at which the configuration that referenced the time range is no longer in effect. The end time and date must be after the start time and date. If no end time and date are specified, the configuration statement is in effect indefinitely.

Format	`absolute [`*`start time date`*`] [`*`end time date`*`]`
Mode	Time-Range Config

no absolute

This command deletes the absolute time entry in the time range

Format	`no absolute`
Mode	Time-Range Config

periodic

Use this command to add a periodic time entry to a time range. The time parameter is based off of the currently configured time zone.

The first occurrence of the days-of-the-week argument is the starting day(s) from which the configuration that referenced the time range starts going into effect. The second occurrence is the ending day or days from which the configuration that referenced the time range is no longer in effect. If the end days-of-the-week are the same as the start, they can be omitted

This argument can be any single day or combinations of days: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday. Other possible values are:

- daily — Monday through Sunday
- weekdays — Monday through Friday
- weekend — Saturday and Sunday

If the ending days of the week are the same as the starting days of the week, they can be omitted.

The first occurrence of the time argument is the starting hours:minutes which the configuration that referenced the time range starts going into effect. The second occurrence is the ending hours:minutes at which the configuration that referenced the time range is no longer in effect.

The hours:minutes are expressed in a 24-hour clock. For example, 8:00 is 8:00 am and 20:00 is 8:00 pm.

Format	`periodic` *`days-of-the-week time`* **`to`** *`time`*
Mode	Time-Range Config

no periodic

This command deletes a periodic time entry from a time range

Format	*`no periodic days-of-the-week time to time`*
Mode	Time-Range Config

show time-range

Use this command to display a time range and all the absolute/periodic time entries that are defined for the time range. Use the name parameter to identify a specific time range to display. When name is not specified, all the time ranges defined in the system are displayed.

Format	`show time-range [name]`
Mode	Privileged EXEC

The information in the following table displays when no time range name is specified.

Column	Meaning
Admin Mode	The administrative mode of the time range feature on the switch
Current number of all Time Ranges	The number of time ranges currently configured in the system.
Maximum number of all Time Ranges	The maximum number of time ranges that can be configured in the system.
Time Range Name	Name of the time range.
Status	Status of the time range (active/inactive)
Periodic Entry count	The number of periodic entries configured for the time range.
Absolute Entry	Whether an absolute entry has been configured for the time range (Exists).

Auto-Voice over IP Commands

This section describes the commands used to configure Auto-Voice over IP (VoIP) commands. The Auto-VoIP feature explicitly matches VoIP streams in Ethernet switches and provides them with a better class-of-service than ordinary traffic. When you enable the Auto-VoIP feature on an interface, the interface scans incoming traffic for the following call-control protocols:

- Session Initiation Protocol (SIP)

- H.323
- Skinny Client Control Protocol (SCCP)

When a call-control protocol is detected, the switch assigns the traffic in that session to the highest *CoS* queue, which is generally used for time-sensitive traffic.

auto-voip

Use this command to configure auto VoIP mode. The supported modes are protocol-based and oui-based. Protocol-based auto VoIP prioritizes the voice data based on the layer 4 port used for the voice session. OUI based auto VoIP prioritizes the phone traffic based on the known OUI of the phone.

When both modes are enabled, if the connected phone OUI is one of the configured OUI, then the voice data is prioritized using OUI Auto VoIP, otherwise protocol-based Auto VoIP is used to prioritize the voice data.

Active sessions are cleared if protocol-based auto VoIP is disabled on the port.

Default	oui-based
Format	`auto-voip [protocol-based | oui-based]`
Mode	• Global Config • Interface Config

no auto-voip

Use the no form of the command to set the default mode.

auto-voip oui

Use this command to configure an OUI for Auto VoIP. The traffic from the configured OUI will get the highest priority over the other traffic. The oui-prefix is a unique OUI that identifies the device manufacturer or vendor. The OUI is specified in three octet values (each octets represented as two hexadecimal digits) separated by colons. The string is a description of the OUI that identifies the manufacturer or vendor associated with the OUI.

Default	A list of known OUIs is present.
Format	`auto-voip oui` *`oui-prefix`* **`desc`** *`string`*
Mode	Global Config

The following example shows how to add an OUI to the table.

```
(Extreme 220) (Config) #auto-voip oui 00:03:6B desc "Cisco VoIPPhone"
```

no auto-voip oui

Use the no form of the command to remove a configured OUI prefix from the table.

Format	`no auto-voip oui oui-prefix`
Mode	Global Config

auto-voip oui-based priority

Use this command to configure the global OUI based auto VoIP priority. If the phone OUI is matches one of the configured OUI, then the priority of traffic from the phone is changed to OUI priority configured through this command. The priority-value is the 802.1p priority used for traffic that matches a value in the known OUI list. If the interface detects an OUI match, the switch assigns the traffic in that session to the traffic class mapped to this priority value. Traffic classes with a higher value are generally used for time-sensitive traffic.

Default	Highest available priority.
Format	`auto-voip oui-based priority` *`priority-value`*
Mode	Global Config

The following example shows how to add an OUI to the table.

```
(Extreme 220) (Config) #auto-voip oui 00:03:6B desc "Cisco VoIPPhone"
```

no auto-voip oui

Use the no form of the command to remove a configured OUI prefix from the table.

Format	`no auto-voip oui` *`oui-prefix`*
Mode	• Global Config • Interface Config

auto-voip protocol-based

Use this command to configure the global protocol-based auto VoIP remarking priority or traffic-class. If remark priority is configured, the voice data of the session is remarked with the priority configured through this command. The remark-priority is the 802.1p priority used for protocol-based VoIP traffic. If the interface detects a call-control protocol, the device marks traffic in that session with the specified 802.1p priority value to ensure voice traffic always gets the highest priority throughout the network path.

The tc value is the traffic class used for protocol-based VoIP traffic. If the interface detects a call-control protocol, the device assigns the traffic in that session to the configured *CoS* queue. Traffic classes with a higher value are generally used for time-sensitive traffic. The CoS queue associated with the specified traffic class should be configured with the appropriate bandwidth allocation to allow priority treatment for VoIP traffic.

Note
You must enable tagging on auto VoIP enabled ports to remark the voice data upon egress.

Default	Traffic class 7
Format	`auto-voip protocol-based {`**`remark`** *`remark-priority`* `|` **`traffic-class`** *`tc`*`}`
Mode	• Global Config • Interface Config

no auto-voip protocol-based

Use this command to reset the global protocol based auto VoIP remarking priority or traffic-class to the default.

Format	`no auto-voip protocol-based {remark remark-priority	traffic-class tc}`
Mode	• Global Config • Interface Config

auto-voip vlan

Use this command to configure the global Auto VoIP VLAN ID. The VLAN behavior is depend on the configured auto VoIP mode. The auto-VoIP VLAN is the VLAN used to segregate VoIP traffic from other non-voice traffic. All VoIP traffic that matches a value in the known OUI list gets assigned to this VoIP VLAN.

Default	None
Format	`auto-voip` **`vlan`** *`vlan-id`*
Mode	Global Config

no auto-voip vlan

Use the no form of the command to reset the auto-VoIP VLAN ID to the default value.

Format	`no auto-voip vlan`
Mode	Global Config

show auto-voip

Use this command to display the auto VoIP settings on the interface or interfaces of the switch.

Format	`show auto-voip {protocol-based|oui-based} interface {`*`unit/slot/port`*`|all}`
Mode	Privileged EXEC

Column	Meaning
VoIP VLAN ID	The global VoIP VLAN ID.
Prioritization Type	The type of prioritization used on voice traffic.
Class Value	• If the Prioritization Type is configured as **traffic-class**, then this value is the queue value. • If the Prioritization Type is configured as **remark**, then this value is 802.1p priority used to remark the voice traffic.
Priority	The 802.1p priority. This field is valid for OUI auto VoIP.
AutoVoIP Mode	The Auto VoIP mode on the interface.

The following example shows CLI display output for the command.

```
(Extreme 220) (Routing)# show auto-voip protocol-based interface all
VoIP VLAN Id..................................... 2
Prioritization Type.............................. traffic-class
Class Value.....................................   7
Interface                  Auto VoIP            Operational Status
                             Mode
---------    -------------- -----------------
0/1           Disabled       Down
0/2           Disabled       Down
0/3           Disabled       Down
0/4           Disabled       Down
```

The following example shows CLI display output for the command.

```
(Extreme 220) (Routing)# show auto-voip oui-based interface all
VoIP VLAN Id..................................... 2
Priority......................................... 7
Interface   Auto VoIP   Operational Status
                Mode
---------  -------------- ------------------
0/1        Disabled       Down
0/2        Disabled       Down
0/3        Disabled       Down
0/4        Disabled       Down
0/5        Disabled       Down
```

show auto-voip oui-table

Use this command to display the VoIP oui-table information.

Format	show auto-voip oui-table
Mode	Privileged EXEC

Column	Meaning
OUI	OUI of the source MAC address.
Status	Default or configured entry.
OUI Description	Description of the OUI.

The following example shows CLI display output for the command.

```
(Extreme 220) (Routing)# show auto-voip oui-table
OUI          Status          Description
---------    ----------     ---------
00:01:E3     Default                                    SIEMENS
00:03:6B     Default                                    CISCO1
00:01:01     Configured                                VoIP phone
```

9 Application Commands

This chapter describes the commands used to install, start, stop, and view applications on the system.

application install

This command makes the application started by the designated executable file available for configuration and execution. The parameters of this command determine how the application is run on the switch.

This command can be issued using an already installed application file name to update the parameters. This updates the configuration for the next time the application is started.

This command can be issued for a file that is not currently on the switch. This allows preconfiguration of the execution parameters. The configuration does not take effect until the executable file is present in the switch file system.

Note
The ExtremeCloud application, `connector.pyz`, is pre-installed on your 200 Series switch and does not need to be installed using this command.

Format	`application install` *`filename`* [**`start-on-boot`**] | [**`auto-restart`**] | [**`cpu-sharing`** *`0-99`*] | [**`max-megabytes`** *`0-200`*]
Mode	Global Config

Parameter	Description
`filename`	The name of the file containing the executable or script that is started as a Linux process for the application.
`start-on-boot`	Starts the application each time the switch boots up. Takes effect on the first reboot after setting. Omit this keyword from the command to disable starting the application at boot time.
`auto-restart`	Automatically restarts the application's process(es) if they stop running. Omit this keyword from the command to disable the automatic restart of the application.

Parameter	Description
cpu-sharing *0–99*	Sets the CPU share allocated to this application, expressed as a percentage between 0 and 99. If 0 is specified, the application process(es) are not limited. If this keyword is not specified, the default value of 0 is used.
max-megabytes *0–200*	Sets the maximum memory resource that the application process(es) can consume. Expressed as megabytes between 0 and 200. If 0 is specified, the application process(es) are not limited. If this keyword is not specified, the default value of 0 is used.

To start an installed application, use the application start on page 662 command.

no application install

This command removes the configuration of an application for execution on the switch. If the application is running, all processes associated with the application are stopped automatically.

Format	`no application install` *`filename`*
Mode	Global Config

For example, to remove the ExtremeCloud application, issue the command:

```
(Extreme 220) (Config) #no application install connector.pyz
```

application start

This command starts the execution of the specified application. Before an application can be started, it must first be installed using the application install on page 661 command. (Exception: the ExtremeCloud application, `connector.pyz`, is pre-installed on your 200 Series switch.)

Format	`application start` *`filename`*
Mode	Privileged EXEC

application stop

This command stops the execution of the specified application.

Format	`application stop` *`filename`*
Mode	Privileged EXEC

show application

This command displays the installed applications and their parameters.

Format	`show application` *`filename`*
Mode	Privileged EXEC

Column	Meaning
Name	The filename for the application.
StartOnBoot	Whether the application is configured to start on boot up: • Yes: The application will start on boot up. • No: The application will not start on boot up.
AutoRestart	Whether the application is configured to restart when the application process ends: • Yes: The application will restart when the application process ends. • No: The application will not restart when the application process ends.
CPU Sharing	The configured application CPU utilization limit expressed as a percentage. `None` if unlimited.
Max Memory	The configured application memory limit in megabytes. `None` if unlimited.

The following example shows the displayed parameters for the ExtremeCloud application.

```
(Extreme 220)# show application connector.pyz
Open application table contains 1 entries.
Name             StartOnBoot    AutoRestart    CPU Sharing   Max Memory   Preload   Version
-------------    -----------    -----------    -----------   ----------   -------
-------------------
connector.pyz    Yes            Yes            20            40           Yes
3.0.23.3
```

show application files

This command displays the files in the application directory of the switch's file system.

Format	`show application files`
Mode	Privileged EXEC

Column	Meaning
filename	The name of the file.
File size	The number of bytes the file occupies in the file system.
Directory size	The number of bytes occupied by all files in the application directory.

10 200 Series Log Messages

This chapter lists common log messages associated with 200 Series switches, along with information regarding the cause of each message. There is no specific action that can be taken per message. When a problem is being diagnosed, a set of these messages in the event log, along with an understanding of the system configuration and details of the problem, will help Extreme Networks determine the root cause of the problem. The most recent log messages are displayed first.

Note
This chapter is not a complete list of all syslog messages.

Core

Table 15: BSP Log Messages

Component	Message	Cause
BSP	Event(0xaaaaaaaa)	Switch has restarted.
BSP	Starting code...	BSP initialization complete, starting 200 Series application.

Table 16: NIM Log Messages

Component	Message	Cause
NIM	NIM: L7_ATTACH out of order for interface unit x slot x port x	Interface creation out of order.
NIM	NIM: Failed to find interface at unit x slot x port x for event(x)	There is no mapping between the USP and Interface number.
NIM	NIM: L7_DETACH out of order for interface unit x slot x port x	Interface creation out of order.
NIM	NIM: L7_DELETE out of order for interface unit x slot x port x	Interface creation out of order.

Table 16: NIM Log Messages (continued)

Component	Message	Cause
NIM	NIM: event(x),intf(x),component(x), in wrong phase	An event was issued to NIM during the wrong configuration phase (probably Phase 1, 2, or WMU).
NIM	NIM: Failed to notify users of interface change	Event was not propagated to the system.
NIM	NIM: failed to send message to NIM message Queue.	NIM message queue full or non-existent.
NIM	NIM: Failed to notify the components of L7_CREATE event	Interface not created.
NIM	NIM: Attempted event (x), on USP x.x.x before phase 3	A component issued an interface event during the wrong initialization phase.
NIM	NIM: incorrect phase for operation	An API call was made during the wrong initialization phase.
NIM	NIM: Component(x) failed on event(x) for interface	A component responded with a fail indication for an interface event.
NIM	NIM: Timeout event(x), interface remainingMask = xxxx	A component did not respond before the NIM timeout occurred.

Table 17: SIM Log Message

Component	Message	Cause
SIM	IP address conflict on service port/network port for IP address x.x.x.x. Conflicting host MAC address is xx:xx:xx:xx:xx:xx	This message appears when an address conflict is detected in the LAN for the service port/network port IP.

Table 18: System Log Messages

Component	Message	Cause
SYSTEM	Configuration file fastpath.cfg size is 0 (zero) bytes	The configuration file could not be read. This message may occur on a system for which no configuration has ever been saved or for which configuration has been erased.
SYSTEM	could not separate SYSAPI_CONFIG_FILENAME	The configuration file could not be read. This message may occur on a system for which no configuration has ever been saved or for which configuration has been erased.
SYSTEM	Building defaults for file *file name* version *version num*	Configuration did not exist or could not be read for the specified feature or file. Default configuration values will be used. The file name and version are indicated.

Table 18: System Log Messages (continued)

Component	Message	Cause
SYSTEM	File *filename*: same version (*version num*) but the sizes (*version size - expected version size*) differ	The configuration file which was loaded was of a different size than expected for the version number. This message indicates the configuration file needed to be migrated to the version number appropriate for the code image. This message may appear after upgrading the code image to a more current release.
SYSTEM	Migrating config file *filename* from version *version num* to *version num*	The configuration file identified was migrated from a previous version number. Both the old and new version number are specified. This message may appear after upgrading the code image to a more current release.
SYSTEM	Building Defaults	Configuration did not exist or could not be read for the specified feature. Default configuration values will be used.
SYSTEM	sysapiCfgFileGet failed size = *expected size of file* version = *expected version*	Configuration did not exist or could not be read for the specified feature. This message is usually followed by a message indicating that default configuration values will be used.

Utilities

Table 19: Trap Mgr Log Message

Component	Message	Cause
Trap Mgr	Link Up/Down: unit/slot/port	An interface changed link state.

Table 20: DHCP Filtering Log Messages

Component	Message	Cause
DHCP (Dynamic Host Configuration Protocol) Filtering	Unable to create r/w lock for DHCP Filtering	Unable to create semaphore used for dhcp filtering configuration structure.
DHCP Filtering	Failed to register with nv Store.	Unable to register save and restore functions for configuration save.
DHCP Filtering	Failed to register with NIM	Unable to register with NIM for interface callback functions.
DHCP Filtering	Error on call to sysapiCfgFileWrite file	Error on trying to save configuration.

Table 21: NVStore Log Messages

Component	Message	Cause
NVStore	Building defaults for file XXX	A component's configuration file does not exist or the file's checksum is incorrect so the component's default configuration file is built.
NVStore	Error on call to osapiFsWrite routine on file XXX	Either the file cannot be opened or the OS's file I/O returned an error trying to write to the file.
NVStore	File XXX corrupted from file system. Checksum mismatch.	The calculated checksum of a component's configuration file in the file system did not match the checksum of the file in memory.
NVStore	Migrating config file XXX from version Y to Z	A configuration file version mismatch was detected so a configuration file migration has started.

Table 22: RADIUS Log Messages

Component	Message	Cause
RADIUS	RADIUS: Invalid data length - xxx	The RADIUS Client received an invalid message from the server.
RADIUS	RADIUS: Failed to send the request	A problem communicating with the RADIUS server.
RADIUS	RADIUS: Failed to send all of the request	A problem communicating with the RADIUS server during transmit.
RADIUS	RADIUS: Could not get the Task Sync semaphore!	Resource issue with RADIUS Client service.
RADIUS	RADIUS: Buffer is too small for response processing	RADIUS Client attempted to build a response larger than resources allow.
RADIUS	RADIUS: Could not allocate accounting requestInfo	Resource issue with RADIUS Client service.
RADIUS	RADIUS: Could not allocate requestInfo	Resource issue with RADIUS Client service.
RADIUS	RADIUS: osapiSocketRecvFrom returned error	Error while attempting to read data from the RADIUS server.
RADIUS	RADIUS: Accounting-Response failed to validate, id = xxx	The RADIUS Client received an invalid message from the server.
RADIUS	RADIUS: User (xxx) needs to respond for challenge	An unexpected challenge was received for a configured user.
RADIUS	RADIUS: Could not allocate a buffer for the packet	Resource issue with RADIUS Client service.
RADIUS	RADIUS: Access-Challenge failed to validate, id = xxx	The RADIUS Client received an invalid message from the server.
RADIUS	RADIUS: Failed to validate Message-Authenticator, id = xxx	The RADIUS Client received an invalid message from the server.
RADIUS	RADIUS: Access-Accept failed to validate, id = xxx	The RADIUS Client received an invalid message from the server.

Table 22: RADIUS Log Messages (continued)

Component	Message	Cause
RADIUS	RADIUS: Invalid packet length – xxx	The RADIUS Client received an invalid message from the server.
RADIUS	RADIUS: Response is missing Message-Authenticator, id = xxx	The RADIUS Client received an invalid message from the server.
RADIUS	RADIUS: Server address doesn't match configured server	RADIUS Client received a server response from an unconfigured server.

Table 23: TACACS+ Log Messages

Component	Message	Cause
TACACS+	TACACS+: authentication error, no server to contact	TACACS+ request needed, but no servers are configured.
TACACS+	TACACS+: connection failed to server x.x.x.x	TACACS+ request sent to server x.x.x.x but no response was received.
TACACS+	TACACS+: no key configured to encrypt packet for server x.x.x.x	No key configured for the specified server.
TACACS+	TACACS+: received invalid packet type from server.	Received packet type that is not supported.
TACACS+	TACACS+: invalid major version in received packet.	Major version mismatch.
TACACS+	TACACS+: invalid minor version in received packet.	Minor version mismatch.

Table 24: LLDP Log Message

Component	Message	Cause
LLDP (Link Layer Discovery Protocol)	lldpTask(): invalid message type:xx. xxxxxx:xx	Unsupported LLDP packet received.

Table 25: SNTP Log Message

Component	Message	Cause
SNTP (Simple Network Time Protocol)	SNTP: system clock synchronized on %s UTC	Indicates that SNTP has successfully synchronized the time of the box with the server.

Table 26: DHCPv6 Client Log Messages

Component	Message	Cause
DHCP6 Client	ip6Map dhcp add failed.	This message appears when the update of a DHCP leased IP address to IP6Map fails.
DHCP6 Client	osapiNetAddrV6Add failed on interface xxx.	This message appears when the update of a DHCP leased IP address to the kernel IP stack fails.
DHCP6 Client	Failed to add DNS Server xxx to DNS Client.	This message appears when the update of a DNS6 Server address given by the DHCPv6 Server to the DNS6 Client fails.
DHCP6 Client	Failed to add Domain name xxx to DNS Client.	This message appears when the update of a DNS6 Domain name info given by the DHCPv6 Server to the DNS6 Client fails.

Table 27: DHCPv4 Client Log Messages

Component	Message	Cause
DHCP4 Client	Unsupported subOption (xxx) in Vendor Specific Option in received DHCP pkt	This message appears when a message is received from the DHCP Server that contains an un-supported Vendor Option.
DHCP4 Client	Failed to acquire an IP address on xxx; DHCP Server did not respond.	This message appears when the DHCP Client fails to lease an IP address from the DHCP Server.
DHCP4 Client	DNS name server entry add failed.	This message appears when the update of a DNS Domain name server info given by the DHCP Server to the DNS Client fails.
DHCP4 Client	DNS domain name list entry addition failed.	This message appears when the update of a DNS Domain name list info given by the DHCP Server to the DNS Client fails.
DHCP4 Client	Interface xxx Link State is Down. Connect the port and try again.	This message appears when the Network protocol is configured with DHCP without any active links in the Management VLAN.

Management

Table 28: SNMP Log Message

Component	Message	Cause
SNMP (Simple Network Management Protocol)	EDB Callback: Unit Join: x.	A new unit has joined the stack.

Table 29: EmWeb Log Messages

Component	Message	Cause
EmWeb	EMWEB (Telnet): Max number of Telnet login sessions exceeded	A user attempted to connect via Telnet when the maximum number of Telnet sessions were already active.
EmWeb	EMWEB (SSH): Max number of SSH login sessions exceeded	A user attempted to connect via SSH when the maximum number of SSH sessions were already active.
EmWeb	Handle table overflow	All the available EmWeb connection handles are being used and the connection could not be made.
EmWeb	ConnectionType EmWeb socket accept() failed: errno	Socket accept failure for the specified connection type.
EmWeb	ewsNetHTTPReceive failure in NetReceiveLoop() - closing connection.	Socket receive failure.
EmWeb	EmWeb: connection allocation failed	Memory allocation failure for the new connection.
EmWeb	EMWEB TransmitPending: EWOULDBLOCK error sending data	Socket error on send.
EmWeb	ewaNetHTTPEnd: internal error - handle not in Handle table	EmWeb handle index not valid.
EmWeb	ewsNetHTTPReceive:recvBufCnt exceeds MAX_QUEUED_RECV_BUFS!	The receive buffer limit has been reached. Bad request or DoS attack.
EmWeb	EmWeb accept: XXXX	Accept function for new SSH connection failed. XXXX indicates the error info.

Table 30: CLI_UTIL Log Messages

Component	Message	Cause
CLI_UTIL	Telnet Send Failed errno = 0x%x	Failed to send text string to the Telnet client.
CLI_UTIL	osapiFsDir failed	Failed to obtain the directory information from a volume's directory.

Table 31: WEB Log Messages

Component	Message	Cause
WEB	Max clients exceeded	This message is shown when the maximum allowed java client connections to the switch is exceeded.
WEB	Error on send to sockfd XXXX, closing connection	Failed to send data to the java clients through the socket.
WEB	# (XXXX) Form Submission Failed. No Action Taken.	The form submission failed and no action is taken. XXXX indicates the file under consideration.

Table 31: WEB Log Messages (continued)

Component	Message	Cause
WEB	ewaFormServe_file_download() - WEB Unknown return code from tftp download result	Unknown error returned while downloading file using TFTP from web interface.
WEB	ewaFormServe_file_upload() - Unknown return code from tftp upload result	Unknown error returned while uploading file using TFTP from web interface.
WEB	Web UI Screen with unspecified access attempted to be brought up	Failed to get application-specific authorization handle provided to EmWeb/Server by the application in ewsAuthRegister(). The specified web page will be served in read-only mode.

Table 32: CLI_WEB_MGR Log Messages

Component	Message	Cause
CLI_WEB_MGR	File size is greater than 2K	The banner file size is greater than 2K bytes.
CLI_WEB_MGR	No. of rows greater than allowed maximum of XXXX	When the number of rows exceeds the maximum allowed rows.

Table 33: SSHD Log Messages

Component	Message	Cause
SSHD	SSHD: Unable to create the global (data) semaphore	Failed to create semaphore for global data protection.
SSHD	SSHD: Msg Queue is full, event = XXXX	Failed to send the message to the SSHD message queue as message queue is full. XXXX indicates the event to be sent.
SSHD	SSHD: Unknown UI event in message, event = XXXX	Failed to dispatch the UI event to the appropriate SSHD function as it's an invalid event. XXXX indicates the event to be dispatched.
SSHD	sshdApiCnfgrCommand: Failed calling sshdIssueCmd.	Failed to send the message to the SSHD message queue.

Table 34: SSLT Log Messages

Component	Message	Cause
SSLT	SSLT: Exceeded maximum, ssltConnectionTask	Exceeded maximum allowed SSLT connections.
SSLT	SSLT: Error creating Secure server socket6	Failed to create secure server socket for IPV6.
SSLT	SSLT: Can't connect to unsecure server at XXXX, result = YYYY, errno = ZZZZ	Failed to open connection to unsecure server. XXXX is the unsecure server socket address. YYYY is the result returned from connect function and ZZZZ is the error code.

Table 34: SSLT Log Messages (continued)

Component	Message	Cause
SSLT	SSLT: Msg Queue is full, event = XXXX	Failed to send the received message to the SSLT message queue as message queue is full. XXXX indicates the event to be sent.
SSLT	SSLT: Unknown UI event in message, event = XXXX	Failed to dispatch the received UI event to the appropriate SSLT function as it's an invalid event. XXXX indicates the event to be dispatched.
SSLT	ssltApiCnfgrCommand: Failed calling ssltIssueCmd.	Failed to send the message to the SSLT message queue.
SSLT	SSLT: Error loading certificate from file XXXX	Failed while loading the SSLcertificate from specified file. XXXX indicates the file from where the certificate is being read.
SSLT	SSLT: Error loading private key from file	Failed while loading private key for SSL connection.
SSLT	SSLT: Error setting cipher list (no valid ciphers)	Failed while setting cipher list.
SSLT	SSLT: Could not delete the SSL semaphores	Failed to delete SSL semaphores during cleanup of all resources associated with the OpenSSL Locking semaphores.

Table 35: User_Manager Log Messages

Component	Message	Cause
User_Manager	User Login Failed for XXXX	Failed to authenticate user login. XXXX indicates the username to be authenticated.
User_Manager	Access level for user XXXX could not be determined. Setting to level 1.	Invalid access level specified for the user. The access level is set to level 1. XXXX indicates the username.
User_Manager	Could not migrate config file XXXX from version YYYY to ZZZZ. Using defaults.	Failed to migrate the config file. XXXX is the config file name. YYYY is the old version number and ZZZZ is the new version number.

Switching

Table 36: Protected Ports Log Messages

Component	Message	Cause
Protected Ports	Protected Port: failed to save configuration	This appears when the protected port configuration cannot be saved.
Protected Ports	protectedPortCnfgrInitPhase1Process: Unable to create r/w lock for protected Port	This appears when protectedPortCfgRWLock Fails.
Protected Ports	protectedPortCnfgrInitPhase2Process: Unable to register for VLAN change callback	This appears when nimRegisterIntfChange with VLAN fails.

Table 36: Protected Ports Log Messages (continued)

Component	Message	Cause
Protected Ports	Cannot add interface xxx to group yyy	This appears when an interface could not be added to a particular group.
Protected Ports	unable to set protected port group	This appears when a dtl call fails to add interface mask at the driver level.
Protected Ports	Cannot delete interface xxx from group yyy	This appears when a dtl call to delete an interface from a group fails.
Protected Ports	Cannot update group YYY after deleting interface XXX	This message appears when an update group for a interface deletion fails.
Protected Ports	Received an interface change callback while not ready to receive it	This appears when an interface change call back has come before the protected port component is ready.

Table 37: IP Subnet VLANS Log Messages

Component	Message	Cause
IP subnet VLANs	ERROR vlanIpSubnetSubnetValid:Invalid subnet	This occurs when an invalid pair of subnet and netmask has come from the CLI.
IP subnet VLANs	IP Subnet Vlans: failed to save configuration	This message appears when save configuration of subnet vlans failed.
IP subnet VLANs	vlanIpSubnetCnfgrInitPhase1Process: Unable to create r/w lock for vlanIpSubnet	This appears when a read/write lock creations fails.
IP subnet VLANs	vlanIpSubnetCnfgrInitPhase2Process: Unable to register for VLAN change callback	This appears when this component unable to register for vlan change notifications.
IP subnet VLANs	vlanIpSubnetCnfgrFiniPhase1Process: could not delete avl semaphore	This appears when a semaphore deletion of this component fails.
IP subnet VLANs	vlanIpSubnetDtlVlanCreate: Failed	This appears when a dtl call fails to add an entry into the table.
IP subnet VLANs	vlanIpSubnetSubnetDeleteApply: Failed	This appears when a dtl fails to delete an entry from the table.
IP subnet VLANs	vlanIpSubnetVlanChangeCallback: Failed to add an Entry	This appears when a dtl fails to add an entry for a vlan add notify event.
IP subnet VLANs	vlanIpSubnetVlanChangeCallback: Failed to delete an Entry	This appears when a dtl fails to delete an entry for an vlan delete notify event.

Table 38: Mac-based VLANs Log Messages

Component	Message	Cause
MAC based VLANs	MAC VLANs: Failed to save configuration	This message appears when save configuration of Mac vlans failed.
MAC based VLANs	vlanMacCnfgrInitPhase1Process: Unable to create r/w lock for vlanMac	This appears when a read/write lock creations fails.
MAC based VLANs	Unable to register for VLAN change callback	This appears when this component unable to register for vlan change notifications.

Table 38: Mac-based VLANs Log Messages (continued)

Component	Message	Cause
MAC based VLANs	vlanMacCnfgrFiniPhase1Process: could not delete avl semaphore	This appears when a semaphore deletion of this component fails.
MAC based VLANs	vlanMacAddApply: Failed to add an entry	This appears when a dtl call fails to add an entry into the table.
MAC based VLANs	vlanMacDeleteApply: Unable to delete an Entry	This appears when a dtl fails to delete an entry from the table.
MAC based VLANs	vlanMacVlanChangeCallback: Failed to add an entry	This appears when a dtl fails to add an entry for a vlan add notify event.
MAC based VLANs	vlanMacVlanChangeCallback: Failed to delete an entry	This appears when a dtl fails to delete an entry for an vlan delete notify event.

Table 39: 802.1X Log Messages

Component	Message	Cause
802.1X	function: Failed calling dot1xIssueCmd	802.1X message queue is full.
802.1X	function: EAP message not received from server	RADIUS server did not send required EAP message.
802.1X	function: Out of System buffers	802.1X cannot process/transmit message due to lack of internal buffers.
802.1X	function: could not set state to *authorized/unauthorized*, intf xxx	DTL call failed setting authorization state of the port.
802.1X	dot1xApplyConfigData: Unable to *enable/disable* dot1x in driver	DTL call failed enabling/disabling 802.1X.
802.1X	dot1xSendRespToServer: dot1xRadiusAccessRequestSend failed	Failed sending message to RADIUS server.
802.1X	dot1xRadiusAcceptProcess: error calling radiusAccountingStart, ifIndex = xxx	Failed sending accounting start to RADIUS server.
802.1X	function: failed sending terminate cause, intf xxx	Failed sending accounting stop to RADIUS server.

Table 40: IGMP Snooping Log Messages

Component	Message	Cause
IGMP (Internet Group Management Protocol) Snooping	function: osapiMessageSend failed	IGMP Snooping message queue is full.
IGMP Snooping	Failed to set global igmp snooping mode to xxx	Failed to set global IGMP Snooping mode due to message queue being full.
IGMP Snooping	Failed to set igmp snooping mode xxx for interface yyy	Failed to set interface IGMP Snooping mode due to message queue being full.

Table 40: IGMP Snooping Log Messages (continued)

Component	Message	Cause
IGMP Snooping	Failed to set igmp mrouter mode xxx for interface yyy	Failed to set interface multicast router mode due to IGMP Snooping message queue being full.
IGMP Snooping	Failed to set igmp snooping mode xxx for vlan yyy	Failed to set VLAN IGM Snooping mode due to message queue being full.
IGMP Snooping	Failed to set igmp mrouter mode%d for interface xxx on Vlan yyy	Failed to set VLAN multicast router mode due to IGMP Snooping message queue being full.
IGMP Snooping	snoopCnfgrInitPhase1Process: Error allocating small buffers	Could not allocate buffers for small IGMP packets.
IGMP Snooping	snoopCnfgrInitPhase1Process: Error allocating large buffers	Could not allocate buffers for large IGMP packets.

Table 41: GARP/GVRP/GMRP Log Messages

Component	Message	Cause
GARP/GVRP/ GMRP	garpSpanState, garpIfStateChange, GarpIssueCmd, garpDot1sChangeCallBack, garpApiCnfgrCommand, garpLeaveAllTimerCallback, garpTimerCallback: QUEUE SEND FAILURE:	The garpQueue is full, logs specifics of the message content like internal interface number, type of message, and so forth.
GARP/GVRP/ GMRP	GarpSendPDU: QUEUE SEND FAILURE	The garpPduQueue is full, logs specific of the GPDU, internal interface number, vlan id, buffer handle, and so forth.
GARP/GVRP/ GMRP	garpMapIntfIsConfigurable, gmrpMapIntfIsConfigurable: Error accessing GARP/GMRP config data for interface %d in garpMapIntfIsConfigurable.	A default configuration does not exist for this interface. Typically a case when a new interface is created and has no preconfiguration.
GARP/GVRP/ GMRP	garpTraceMsgQueueUsage: garpQueue usage has exceeded fifty/eighty/ninety percent	Traces the build up of message queue. Helpful in determining the load on GARP.
GARP/GVRP/ GMRP	gid_destroy_port: Error Removing port %d registration for vlan-mac %d - %02X:%02X: %02X:%02X:%02X:%02X	Mismatch between the gmd (gmrp database) and MFDB.
GARP/GVRP/ GMRP	gmd_create_entry: GMRP failure adding MFDB entry: vlan %d and address %s	MFDB table is full.

Table 42: 802.3ad Log Messages

Component	Message	Cause
802.3ad	dot3adReceiveMachine: received default event %x	Received a *LAG (Link Aggregation Group)* PDU and the RX state machine is ignoring this LAGPDU.
802.3ad	dot3adNimEventCompletionCallback, dot3adNimEventCreateCompletionCallback: DOT3AD: notification failed for event(%d), intf(%d), reason(%d)	The event sent to NIM was not completed successfully.

Table 43: FDB Log Message

Component	Message	Cause
FDB (forwarding database)	fdbSetAddressAgingTimeOut: Failure setting fid %d address aging timeout to %d	Unable to set the age time in the hardware.

Table 44: Double VLAN Tag Log Message

Component	Message	Cause
Double Vlan Tag	dvlantagIntfIsConfigurable: Error accessing dvlantag config data for interface %d	A default configuration does not exist for this interface. Typically a case when a new interface is created and has no preconfiguration.

Table 45: IPv6 Provisioning Log Message

Component	Message	Cause
IPV6 Provisioning	ipv6ProvIntfIsConfigurable: Error accessing IPv6 Provisioning config data for interface %d	A default configuration does not exist for this interface. Typically a case when a new interface is created and has no preconfiguration.

Table 46: MFDB Log Message

Component	Message	Cause
MFDB	mfdbTreeEntryUpdate: entry does not exist	Trying to update a non existing entry.

Table 47: 802.1Q Log Messages

Component	Message	Cause
802.1Q	dot1qIssueCmd: Unable to send message %d to dot1qMsgQueue for vlan %d - %d msgs in queue	dot1qMsgQueue is full.
802.1Q	dot1qVlanCreateProcess: Attempt to create a vlan with an invalid vlan id %d ; VLAN %d not in range,	This accommodates for reserved vlan IDs: 4094 - x.
802.1Q	dot1qMapIntfIsConfigurable: Error accessing DOT1Q config data for interface %d in dot1qMapIntfIsConfigurable.	A default configuration does not exist for this interface. Typically a case when a new interface is created and has no preconfiguration.
802.1Q	dot1qVlanDeleteProcess: Deleting the default VLAN	Typically encountered during clear Vlan and clear config.
802.1Q	dot1qVlanMemberSetModify, dot1qVlanTaggedMemberSetModify: Dynamic entry %d can only be modified after it is converted to static	If this vlan is a learnt via GVRP then we cannot modify its member set via management.
802.1Q	dtl failure when adding ports to vlan id %d - portMask = %s	Failed to add the ports to VLAN entry in hardware.

Table 47: 802.1Q Log Messages (continued)

Component	Message	Cause
802.1Q	dtl failure when deleting ports from vlan id %d - portMask = %s	Failed to delete the ports for a VLAN entry from the hardware.
802.1Q	dtl failure when adding ports to tagged list for vlan id %d - portMask = %s	Failed to add the port to the tagged list in hardware.
802.1Q	dtl failure when deleting ports from tagged list for vlan id %d - portMask = %s"	Failed to delete the port to the tagged list from the hardware.
802.1Q	dot1qTask: unsuccessful return code on receive from dot1qMsgQueue: %08x"	Failed to receive the dot1q message from dot1q message queue.
802.1Q	Unable to apply VLAN creation request for VLAN ID %d, Database reached MAX VLAN count!	Failed to create VLAN ID, VLAN Database reached maximum values.
802.1Q	Attempt to create a vlan (%d) that already exists	Creation of the existing Dynamic VLAN ID from the CLI.
802.1Q	DTL call to create VLAN %d failed with rc %d"	Failed to create VLAN ID in hardware.
802.1Q	Problem unrolling data for VLAN %d	Failed to delete VLAN from the VLAN database after failure of VLAN hardware creation.
802.1Q	VLan %d does not exist	Failed to delete VLAN entry.
802.1Q	VLan %d requestor type %d does not exist	Failed to delete dynamic VLAN ID if the given requestor is not valid.
802.1Q	Can not delete the VLAN, Some unknown component has taken the ownership!	Failed to delete, as some unknown component has taken the ownership.
802.1Q	Not valid permission to delete the VLAN %d requestor %d	Failed to delete the VLAN ID as the given requestor and VLAN entry status are not same.
802.1Q	VLAN Delete Call failed in driver for vlan %d	Failed to delete VLAN ID from the hardware.
802.1Q	Problem deleting data for VLAN %d	Failed to delete VLAN ID from the VLAN database.
802.1Q	Dynamic entry %d can only be modified after it is converted to static	Failed to modify the VLAN group filter
802.1Q	Cannot find vlan %d to convert it to static	Failed to convert Dynamic VLAN to static VLAN. VLAN ID not exists.
802.1Q	Only Dynamically created VLANs can be converted	Error while trying to convert the static created VLAN ID to static.
802.1Q	Cannot modify tagging of interface %s to non existence vlan %d"	Error for a given interface sets the tagging property for all the VLANs in the vlan mask.
802.1Q	Error in updating data for VLAN %d in VLAN database	Failed to add VLAN entry into VLAN database.
802.1Q	DTL call to create VLAN %d failed with rc %d	Failed to add VLAN entry in hardware.
802.1Q	Not valid permission to delete the VLAN %d	Failed to delete static VLAN ID. Invalid requestor.
802.1Q	Attempt to set access vlan with an invalid vlan id %d	Invalid VLAN ID.

Table 47: 802.1Q Log Messages (continued)

Component	Message	Cause
802.1Q	Attempt to set access vlan with (%d) that does not exist	VLAN ID not exists.
802.1Q	VLAN create currently underway for VLAN ID %d	Creating a VLAN which is already under process of creation.
802.1Q	VLAN ID %d is already exists as static VLAN	Trying to create already existing static VLAN ID.
802.1Q	Cannot put a message on dot1q msg Queue, Returns:%d	Failed to send Dot1q message on Dot1q message Queue.
802.1Q	Invalid dot1q Interface: %s	Failed to add VLAN to a member of port.
802.1Q	Cannot set membership for user interface %s on management vlan %d	Failed to add VLAN to a member of port.
802.1Q	Incorrect tagmode for vlan tagging. tagmode: %d Interface: %s	Incorrect tagmode for VLAN tagging.
802.1Q	Cannot set tagging for interface %d on non existent VLAN %d"	The VLAN ID does not exist.
802.1Q	Cannot set tagging for interface %d which is not a member of VLAN %d	Failure in Setting the tagging configuration for a interface on a range of VLAN.
802.1Q	VLAN create currently underway for VLAN ID %d"	Trying to create the VLAN ID which is already under process of creation.
802.1Q	VLAN ID %d already exists	Trying to create the VLAN ID which is already exists.
802.1Q	Failed to delete, Default VLAN %d cannot be deleted	Trying to delete Default VLAN ID.
802.1Q	Failed to delete, VLAN ID %d is not a static VLAN	Trying to delete Dynamic VLAN ID from CLI.
802.1Q	Requestor %d attempted to release internal VLAN %d: owned by %d	-

Table 48: 802.1S Log Messages

Component	Message	Cause
802.1S	dot1sIssueCmd: Dot1s Msg Queue is full!!!! Event: %u, on interface: %u, for instance: %u	The message Queue is full.
802.1S	dot1sStateMachineRxBpdu(): Rcvd BPDU Discarded	The current conditions, like port is not enabled or we are currently not finished processing another BPDU on the same interface, does not allow us to process this BPDU.
802.1S	dot1sBpduTransmit(): could not get a buffer	Out of system buffers.

Table 49: Port Mac Locking Log Message

Component	Message	Cause
Port Mac Locking	pmlMapIntfIsConfigurable: Error accessing PML config data for interface %d in pmlMapIntfIsConfigurable.	A default configuration does not exist for this interface. Typically a case when a new interface is created and has no preconfiguration.

Table 50: Protocol-based VLANs Log Messages

Component	Message	Cause
Protocol Based VLANs	pbVlanCnfgrInitPhase2Process: Unable to register NIM callback	Appears when nimRegisterIntfChange fails to register pbVlan for link state changes.
Protocol Based VLANs	pbVlanCnfgrInitPhase2Process: Unable to register pbVlan callback with VLANs	Appears when VLANRegisterForChange fails to register pbVlan for VLAN changes.
Protocol Based VLANs	pbVlanCnfgrInitPhase2Process: Unable to register pbVlan callback with nvStore	Appears when nvStoreRegister fails to register save and restore functions for configuration save.

QoS

Table 51: ACL Log Messages

Component	Message	Cause
ACL (Access Control List)	Total number of ACL rules (x) exceeds max (y) on intf i.	The combination of all ACLs applied to an interface has resulted in requiring more rules than the platform supports.
ACL	aclLogTask: error logging ACL rule trap for correlator number	The system was unable to send an *SNMP* trap for this ACL rule which contains a logging attribute.
ACL	IP ACL number: Forced truncation of one or more rules during config migration	While processing the saved configuration, the system encountered an ACL with more rules than is supported by the current version. This may happen when code is updated to a version supporting fewer rules per ACL than the previous version.

Table 52: CoS Log Message

Component	Message	Cause
COS	cosCnfgrInitPhase3Process: Unable to apply saved config -- using factory defaults	The CoS component was unable to apply the saved configuration and has initialized to the factory default settings.

Table 53: DiffServ Log Messages

Component	Message	Cause
DiffServ	diffserv.c 165: diffServRestore Failed to reset DiffServ. Recommend resetting device	While attempting to clear the running configuration an error was encountered in removing the current settings. This can lead to an inconsistent state in the system. We recommend rebooting the switch.
DiffServ	Policy invalid for service intf: policy name, interface x, direction y	The DiffServ policy definition is not compatible with the capabilities of the interface specified. Check the platform release notes for information on configuration limitations.

Routing/IPv6 Routing

Table 54: DHCP Relay Log Messages

Component	Message	Cause
DHCP relay	REQUEST hops field more than config value	The DHCP relay agent has processed a DHCP request whose HOPS field is larger than the maximum value allowed. The relay agent will not forward a message with a hop count greater than 4.
DHCP relay	Request's seconds field less than the config value	The DHCP relay agent has processed a DHCP request whose SECS field is larger than the configured minimum wait time allowed.
DHCP relay	processDhcpPacket: invalid DHCP packet type: %u\n	The DHCP relay agent has processed an invalid DHCP packet. Such packets are discarded by the relay agent.

Table 55: OSPFv2 Log Messages

Component	Message	Cause
OSPFv2	Best route client deregistration failed for OSPF Redist	OSPFv2 registers with the IPv4 routing table manager (“RTO”) to be notified of best route changes. There are cases where OSPFv2 deregisters more than once, causing the second deregistration to fail. The failure is harmless.
OSPFv2	XX_Call() failure in _checkTimers for thread 0x869bcc0	An OSPFv2 timer has fired but the message queue that holds the event has filled up. This is normally a fatal error.
OSPFv2	Warning: OSPF LSDB is 90% full (22648 LSAs).	OSPFv2 limits the number of Link State Advertisements (LSAs) that can be stored in the link state database (LSDB). When the database becomes 90 or 95 percent full, OSPFv2 logs this warning. The warning includes the current size of the database.

Table 55: OSPFv2 Log Messages (continued)

Component	Message	Cause
OSPFv2	The number of LSAs, 25165, in the OSPF LSDB has exceeded the LSDB memory allocation.	When the OSPFv2 LSDB becomes full, OSPFv2 logs this message. OSPFv2 reoriginates its router LSAs with the metric of all non-stub links set to the maximum value to encourage other routers to not compute routes through the overloaded router.
OSPFv2	Dropping the DD packet because of MTU mismatch	OSPFv2 ignored a Database Description packet whose MTU is greater than the IP MTU on the interface where the DD was received.
OSPFv2	LSA Checksum error in LsUpdate, dropping LSID 1.2.3.4 checksum 0x1234.	OSPFv2 ignored a received link state advertisement (LSA) whose checksum was incorrect.

Table 56: OSPFv3 Log Messages

Component	Message	Cause
OSPFv3 (Open Shortest Path First version 3)	Best route client deregistration failed for OSPFv3 Redist	OSPFv3 registers with the IPv6 routing table manager (“RTO6”) to be notified of best route changes. There are cases where OSPFv3 deregisters more than once, causing the second deregistration to fail. The failure is harmless.
OSPFv3	Warning: OSPF LSDB is 90% full (15292 LSAs).	OSPFv3 limits the number of Link State Advertisements (LSAs) that can be stored in the link state database (LSDB). When the database becomes 90 or 95 percent full, OSPFv3 logs this warning. The warning includes the current size of the database.
OSPFv3	The number of LSAs, 16992, in the OSPF LSDB has exceeded the LSDB memory allocation.	When the OSPFv3 LSDB becomes full, OSPFv3 logs this message. OSPFv3 reoriginates its router LSAs with the R-bit clear indicating that OSPFv3 is overloaded.
OSPFv3	LSA Checksum error detected for LSID 1.2.3.4 checksum 0x34f5. OSPFv3 Database may be corrupted.	OSPFv3 periodically verifies the checksum of each LSA in memory. OSPFv3 logs this.

Table 57: Routing Table Manager Log Messages

Component	Message	Cause
RTO	RTO is no longer full. Routing table contains xxx best routes, xxx total routes, xxx reserved local routes.	When the number of best routes drops below full capacity, RTO logs this notice. The number of bad adds may give an indication of the number of route adds that failed while RTO was full, but a full routing table is only one reason why this count is incremented.
RTO	RTO is full. Routing table contains xxx best routes, xxx total routes, xxx reserved local routes. The routing table manager stores a limited number of best routes. The count of total routes includes alternate routes, which are not installed in hardware.	The routing table manager, also called "RTO," stores a limited number of best routes, based on hardware capacity. When the routing table becomes full, RTO logs this alert. The count of total routes includes alternate routes, which are not installed in hardware.

Table 58: VRRP Log Messages

Component	Message	Cause
VRRP	VRRP packet of size xxx dropped. Min VRRP packet size is xxx; Max VRRP packet size is xxx.	This message appears when there is flood of VRRP messages in the network.
VRRP	VR xxx on interface xxx started as xxx.	This message appears when the *virtual router (VR)* is started in the role of a Master or a Backup.
VRRP	This router is the IP address owner for virtual router xxx on interface xxx. Setting the virtual router priority to xxx.	This message appears when the address ownership status for a specific VR is updated. If this router is the address owner for the VR, set the VR's priority to MAX priority (as per RFC 3768). If the router is no longer the address owner, revert the priority.

Table 59: ARP Log Message

Component	Message	Cause
ARP	IP address conflict on interface xxx for IP address yyy. Conflicting host MAC address is zzz.	When an address conflict is detected for any IP address on the switch upon reception of ARP packet from another host or router.

Table 60: RIP Log Message

Component	Message	Cause
RIP (Routing Information Protocol)	RIP: discard response from xxx via unexpected interface	When RIP response is received with a source address not matching the incoming interface's subnet.

Stacking

Table 61: EDB Log Message

Component	Message	Cause
EDB	EDB Callback: Unit Join: *num*.	Unit *num* has joined the stack.

Technologies

Table 62: General 200 Series Error Messages

Component	Message	Cause
200 Series	Invalid USP unit = x, slot = x, port = x	A port was not able to be translated correctly during the receive.
200 Series	In hapiBroadSystemMacAddress call to 'bcm_l2_addr_add' - FAILED : x	Failed to add an L2 address to the MAC table. This should only happen when a hash collision occurs or the table is full.
200 Series	Failed installing mirror action - rest of the policy applied successfully	A previously configured probe port is not being used in the policy. The release notes state that only a single probe port can be configured.
200 Series	Policy x does not contain rule x	The rule was not added to the policy due to a discrepancy in the rule count for this specific policy. Additionally, the message can be displayed when an old rule is being modified, but the old rule is not in the policy.
200 Series	ERROR: policy x, tmpPolicy x, size x, data x x x x x x x	An issue installing the policy due to a possible duplicate hash.
200 Series	*ACL* x not found in internal table	Attempting to delete a non-existent ACL.
200 Series	ACL internal table overflow	Attempting to add an ACL to a full table.
200 Series	In hapiBroadQosCosQueueConfig, Failed to configure minimum bandwidth. Available bandwidth x	Attempting to configure the bandwidth beyond it's capabilities.
200 Series	USL: failed to put sync response on queue	A response to a sync request was not enqueued. This could indicate that a previous sync request was received after it was timed out.
200 Series	USL: failed to sync ipmc table on unit = x	Either the transport failed or the message was dropped.
200 Series	usl_task_ipmc_msg_send(): failed to send with x	Either the transport failed or the message was dropped.
200 Series	USL: No available entries in the STG table	The Spanning Tree Group table is full in USL.
200 Series	USL: failed to sync stg table on unit = x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued.

Table 62: General 200 Series Error Messages (continued)

Component	Message	Cause
200 Series	USL: A Trunk doesn't exist in USL	Attempting to modify a Trunk that doesn't exist.
200 Series	USL: A Trunk being created by bcmx already existed in USL	Possible synchronization issue between the application, hardware, and sync layer.
200 Series	USL: A Trunk being destroyed doesn't exist in USL	Possible synchronization issue between the application, hardware, and sync layer.
200 Series	USL: A Trunk being set doesn't exist in USL	Possible synchronization issue between the application, hardware, and sync layer.
200 Series	USL: failed to sync trunk table on unit = x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued.
200 Series	USL: Mcast entry not found on a join	Possible synchronization issue between the application, hardware, and sync layer.
200 Series	USL: Mcast entry not found on a leave	Possible synchronization issue between the application, hardware, and sync layer.
200 Series	USL: failed to sync dVLAN data on unit = x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued.
200 Series	USL: failed to sync policy table on unit = x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued.
200 Series	USL: failed to sync VLAN table on unit = x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued.
200 Series	Invalid *LAG* id x	Possible synchronization issue between the BCM driver and HAPI.
200 Series	Invalid uport calculated from the BCM uport bcmx_l2_addr->lport = x	Uport not valid from BCM driver.
200 Series	Invalid USP calculated from the BCM uport \nbcmx_l2_addr->lport = x	USP not able to be calculated from the learn event for BCM driver.
200 Series	Unable to insert route R/P	Route R with prefix P could not be inserted in the hardware route table. A retry will be issued.
200 Series	Unable to Insert host H	Host H could not be inserted in hardware host table. A retry will be issued.
200 Series	USL: failed to sync L3 Intf table on unit = x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued.
200 Series	USL: failed to sync L3 Host table on unit = x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued.
200 Series	USL: failed to sync L3 Route table on unit = x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued.

Table 62: General 200 Series Error Messages (continued)

Component	Message	Cause
200 Series	USL: failed to sync initiator table on unit = x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued.
200 Series	USL: failed to sync terminator table on unit = x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued.
200 Series	USL: failed to sync ip-multicast table on unit = x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued.

O/S Support

Table 63: Linux BSP Log Message

Component	Message	Cause
Linux BSP	rc = 10	Second message logged at bootup, right after Starting code.... Always logged.

Table 64: OSAPI Linux Log Messages

Component	Message	Cause
OSAPI Linux	osapiNetLinkNeighDump: could not open socket! - or – ipstkNdpFlush: could not open socket! – or – osapiNetlinkDumpOpen: unable to bind socket! errno = XX	Couldn't open a NetLink socket. Make sure "ARP Daemon support" (CONFIG_ARPD) is enabled in the Linux kernel, if the reference kernel binary is not being used.
OSAPI Linux	ipstkNdpFlush: sending delete failed	Failed when telling the kernel to delete a neighbor table entry (the message is incorrect).
OSAPI Linux	unable to open /proc/net/ipv6/conf/default/hop_limit	IPv6 MIB objects read, but /proc file system is not mounted, or running kernel does not have IPV6 support.
OSAPI Linux	osapimRouteEntryAdd, errno XX adding 0xYY to ZZ – or – osapimRouteEntryDelete, errno XX deleting 0xYY from ZZ	Error adding or deleting an IPv4 route (listed in hex as YY), on the interface with Linux name ZZ Error code can be looked up in errno.h.
OSAPI Linux	l3intfAddRoute: Failed to Add Route – or – l3intfDeleteRoute: Failed to Delete Route	Error adding or deleting a default gateway in the kernel's routing table (the function is really osapiRawMRouteAdd()/Delete()).
OSAPI Linux	osapiNetIfConfig: ioctl on XX failed: addr: 0xYY, err: ZZ – or – osapiNetIPSet: ioctl on XX failed: addr: 0x%YY	Failed trying to set the IP address (in hex as YY) of the interface with Linux name XX, and the interface does not exist. Sometimes this is a harmless race condition (for example, we try to set address 0 when DHCPing on the network port (dtl0) at bootup, before it's created using TAP).

Table 64: OSAPI Linux Log Messages (continued)

Component	Message	Cause
OSAPI Linux	ping: sendto error	Trouble sending an *ICMP (Internet Control Message Protocol)* echo request packet for the UI ping command. Maybe there was no route to that network.
OSAPI Linux	Failed to Create Interface	Out of memory at system initialization time.
OSAPI Linux	TAP Unable to open XX	The /dev/tap file is missing, or, if not using the reference kernel binary, the kernel is missing "Universal TUN/TAP device driver support" (CONFIG_TUN).
OSAPI Linux	Tap monitor task is spinning on select failures – then – Tap monitor select failed: XX	Trouble reading the /dev/tap device, check the error message XX for details.
OSAPI Linux	Log_Init: log file error - creating new log file	This pertains to the "event log" persistent file in flash. Either it did not exist, or had a bad checksum.
OSAPI Linux	Log_Init: Flash (event) log full; erasing	Event log file has been cleared; happens at boot time.
OSAPI Linux	Log_Init: Corrupt event log; erasing	Event log file had a non-blank entry after a blank entry; therefore, something was messed up.
OSAPI Linux	Failed to Set Interface IP Address – or – IP Netmask – or – Broadcast Address – or – Flags – or – Hardware Address – or – Failed to Retrieve Interface Flags	Trouble adding VRRP IP or MAC address(es) to a Linux network interface.

Glossary

ABR

In OSPF, an Area Border Router has interfaces in multiple areas, and it is responsible for exchanging summary advertisements with other ABRs.

ACL

An Access Control List is a mechanism for filtering packets at the hardware level. Packets can be classified by characteristics such as the source or destination MAC, IP address, IP type, or QoS queue. Once classified, the packets can be forwarded, counted, queued, or dropped.

ad hoc mode

An 802.11 networking framework in which devices or stations communicate directly with each other, without the use of an AP.

ARP

Address Resolution Protocol is part of the TCP/IP suite used to dynamically associate a device's physical address (MAC address) with its logical address (IP address). The system broadcasts an ARP request, containing the IP address, and the device with that IP address sends back its MAC address so that traffic can be transmitted.

ATM

Asynchronous Transmission Mode is a start/stop transmission in which each character is preceded by a start signal and followed by one or more stop signals. A variable time interval can exist between characters. ATM is the preferred technology for the transfer of images.

BGP

Border Gateway Protocol is a router protocol in the IP suite designed to exchange network reachability information with BGP systems in other autonomous systems. You use a fully meshed configuration with BGP.

BGP provides routing updates that include a network number, a list of ASs that the routing information passed through, and a list of other path attributes. BGP works with cost metrics to choose the best available path; it sends updated router information only when one host has detected a change, and only the affected part of the routing table is sent.

BGP communicates within one AS using Interior BGP (IBGP) because BGP does not work well with IGP. Thus the routers inside the AS maintain two routing tables: one for the IGP and one for IBGP. BGP uses exterior BGP (EBGP) between different autonomous systems.

BSS

Basic Service Set is a wireless topology consisting of one access point connected to a wired network and a set of wireless devices. Also called an infrastructure network. See also *IBSS (Independent Basic Service Set)*.

CHAP

Challenge-Handshake Authentication Protocol is one of the two main authentication protocols used to verify a user's name and password for PPP Internet connections. CHAP is more secure because it

performs a three-way handshake during the initial link establishment between the home and remote machines. It can also repeat the authentication anytime after the link has been established.

CoS

Class of Service specifies the service level for the classified traffic type.

DHCP

Dynamic Host Configuration Protocol allows network administrators to centrally manage and automate the assignment of IP addresses on the corporate network. DHCP sends a new IP address when a computer is plugged into a different place in the network. The protocol supports static or dynamic IP addresses and can dynamically reconfigure networks in which there are more computers than there are available IP addresses.

DoS attack

Denial of Service attacks occur when a critical network or computing resource is overwhelmed so that legitimate requests for service cannot succeed. In its simplest form, a DoS attack is indistinguishable from normal heavy traffic. ExtremeXOS software has configurable parameters that allow you to defeat DoS attacks.

DSSS

Direct-Sequence Spread Spectrum is a transmission technology used in Local Area Wireless Network (LAWN) transmissions where a data signal at the sending station is combined with a higher data rate bit sequence, or chipping code, that divides the user data according to a spreading ratio. The chipping code is a redundant bit pattern for each bit that is transmitted, which increases the signal's resistance to interference. If one or more bits in the pattern are damaged during transmission, the original data can be recovered due to the redundancy of the transmission. (Compare with *FHSS (Frequency-Hopping Spread Spectrum)*.)

EAP-TLS/EAP-TTLS

EAP-TLS Extensible Authentication Protocol - Transport Layer Security. A general protocol for authentication that also supports multiple authentication methods, such as token cards, Kerberos, one-time passwords, certificates, public key authentication and smart cards.

IEEE 802.1x specifies how EAP should be encapsulated in LAN frames.
In wireless communications using EAP, a user requests connection to a WLAN through an access point, which then requests the identity of the user and transmits that identity to an authentication server such as RADIUS The server asks the access point for proof of identity, which the access point gets from the user and then sends back to the server to complete the authentication.

EAP-TLS provides for certificate-based and mutual authentication of the client and the network. It relies on client-side and server-side certificates to perform authentication and can be used to dynamically generate user-based and session-based WEP keys.

EAP-TTLS (Tunneled Transport Layer Security) is an extension of EAP-TLS to provide certificate-based, mutual authentication of the client and network through an encrypted tunnel, as well as to generate dynamic, per-user, per-session WEP keys. Unlike EAP-TLS, EAP-TTLS requires only server-side certificates.
(See also *PEAP (Protected Extensible Authentication Protocol)*.)

ECMP

Equal Cost Multi Paths is a routing algorithm that distributes network traffic across multiple high-bandwidth OSPF, BPG, IS-IS, and static routes to increase performance. The Extreme Networks implementation supports multiple equal cost paths between points and divides traffic evenly among the available paths.

ESRP

Extreme Standby Router Protocol is an Extreme Networks-proprietary protocol that provides redundant Layer 2 and routing services to users.

FDB

The switch maintains a database of all MAC address received on all of its ports and uses this information to decide whether a frame should be forwarded or filtered. Each forwarding database (FDB) entry consists of the MAC address of the sending device, an identifier for the port on which the frame was received, and an identifier for the VLAN to which the device belongs. Frames destined for devices that are not currently in the FDB are flooded to all members of the VLAN. For some types of entries, you configure the time it takes for the specific entry to age out of the FDB.

FHSS

Frequency-Hopping Spread Spectrum is a transmission technology used in Local Area Wireless Network (LAWN) transmissions where the data signal is modulated with a narrowband carrier signal that 'hops' in a random but predictable sequence from frequency to frequency as a function of time over a wide band of frequencies. This technique reduces interference. If synchronized properly, a single logical channel is maintained. (Compare with *DSSS (Direct-Sequence Spread Spectrum)*.)

HTTP

Hypertext Transfer Protocol is the set of rules for transferring files (text, graphic images, sound, video, and other multimedia files) on the worldwide web. A web browser makes use of HTTP. HTTP is an application protocol that runs on top of the TCP/IP suite of protocols. (RFC 2616: Hypertext Transfer Protocol -- HTTP/1.1)

HTTPS

Hypertext Transfer Protocol over Secure Socket Layer, or HTTP over SSL, is a web protocol that encrypts and decrypts user page requests as well as the pages that are returned by the web server. HTTPS uses SSL as a sublayer under its regular HTTP application layering. (HTTPS uses port 443 instead of HTTP port 80 in its interactions with the lower layer, TCP/IP.) SSL uses a 40-bit key size for the RC4 stream encryption algorithm, which is considered an adequate degree of encryption for commercial exchange.

IBSS

An IBSS is the 802.11 term for an ad hoc network. See *ad hoc mode*.

ICMP

Internet Control Message Protocol is the part of the TCP/IP protocol that allows generation of error messages, test packets, and operating messages. For example, the ping command allows you to send ICMP echo messages to a remote IP device to test for connectivity. ICMP also supports traceroute, which identifies intermediate hops between a given source and destination.

IGMP

Hosts use Internet Group Management Protocol to inform local routers of their membership in multicast groups. Multicasting allows one computer on the Internet to send content to multiple other computers

that have identified themselves as interested in receiving the originating computer's content. When all hosts leave a group, the router no longer forwards packets that arrive for the multicast group.

LAG

A Link Aggregation Group is the logical high-bandwidth link that results from grouping multiple network links in link aggregation (or load sharing). You can configure static LAGs or dynamic LAGs (using the LACP).

LLDP

Link Layer Discovery Protocol conforms to IEEE 802.1ab and is a neighbor discovery protocol. Each LLDP-enabled device transmits information to its neighbors, including chassis and port identification, system name and description, VLAN names, and other selected networking information. The protocol also specifies timing intervals in order to ensure current information is being transmitted and received.

MD5

Message-Digest algorithm is a hash function that is commonly used to generate a 128-bit hash value. It was designed by Ron Rivest in 1991. MD5 is officially defined in RFC 1321 - The MD5 Message-Digest Algorithm.

MIC

Message Integrity Check (or Code), also called 'Michael', is part of WPA and TKIP. The MIC is an additional 8-byte code inserted before the standard 4-byte ICV appended in by standard WEP to the 802.11 message. This greatly increases the difficulty in carrying out forgery attacks.
Both integrity check mechanisms are calculated by the receiver and compared against the values sent by the sender in the frame. If the values match, there is assurance that the message has not been tampered with.

MLAG

The Multi-switch Link Aggregation Group feature allows users to combine ports on two switches to form a single logical connection to another network device. The other network device can be either a server or a switch that is separately configured with a regular LAG (or appropriate server port teaming) to form the port aggregation.

MSTP

Multiple Spanning Tree Protocol, based on IEEE 802.1Q-2003 (formerly known as IEEE 892.1s), allows you to bundle multiple VLANs into one STP topology, which also provides enhanced loop protection and better scaling. MSTP uses RSTP as the converging algorithm and is compatible with legacy STP protocols.

netmask

A netmask is a string of 0s and 1s that mask, or screen out, the network part of an IP address, so that only the host computer part of the address remains. A frequently-used netmask is 255.255.255.0, used for a Class C subnet (one with up to 255 host computers). The ".0" in the netmask allows the specific host computer address to be visible.

OSPF

An interior gateway routing protocol for TCP/IP networks, Open Shortest Path First uses a link state routing algorithm that calculates routes for packets based on a number of factors, including least hops, speed of transmission lines, and congestion delays. You can also configure certain cost metrics for the

algorithm. This protocol is more efficient and scalable than vector-distance routing protocols. OSPF features include least-cost routing, ECMP routing, and load balancing. Although OSPF requires CPU power and memory space, it results in smaller, less frequent router table updates throughout the network. This protocol is more efficient and scalable than vector-distance routing protocols.

OSPFv3

Open Shortest Path First version 3 is one of the routing protocols used with IPV6 and is similar to OSPF.

PEAP

Protected Extensible Authentication Protocol is an IETF draft standard to authenticate wireless LAN clients without requiring them to have certificates. In PEAP authentication, first the user authenticates the authentication server, then the authentication server authenticates the user. If the first phase is successful, the user is then authenticated over the SSL tunnel created in phase one using EAP-Generic Token Card (EAP-GTC) or Microsoft Challenged Handshake Protocol Version 2 (MSCHAP V2). (See also *EAP-TLS/EAP-TTLS*.)

PoE

The Power over Ethernet standard (IEEE 802.3af) defines how power can be provided to network devices over existing Ethernet connections, eliminating the need for additional external power supplies.

QoS

Quality of Service is a technique that is used to manage network resources and guarantee a bandwidth relationship between individual applications or protocols. A communications network transports a multitude of applications and data, including high-quality video and delay-sensitive data such as real-time voice. Networks must provide secure, predictable, measurable, and sometimes guaranteed services. Achieving the required QoS becomes the secret to a successful end-to-end business solution.

RADIUS

RADIUS is a client/server protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. RADIUS allows a company to maintain user profiles in a central database that all remote servers can share. It provides better security, allowing a company to set up a policy that can be applied at a single administered network point. With RADIUS, you can track usage for billing and for keeping network statistics.

RIP

This IGP vector-distance routing protocol is part of the TCP/IP suite and maintains tables of all known destinations and the number of hops required to reach each. Using Routing Information Protocol, routers periodically exchange entire routing tables. RIP is suitable for use only as an IGP.

SNMP

Simple Network Management Protocol is a standard that uses a common software agent to remotely monitor and set network configuration and runtime parameters. SNMP operates in a multivendor environment, and the agent uses MIBs, which define what information is available from any manageable network device. You can also set traps using SNMP, which send notifications of network events to the system log.

SNTP

Simple Network Time Protocol is used to synchronize the system clocks throughout the network. An extension of NTP, SNTP can usually operate with a single server and allows for IPv6 addressing.

SSL

Secure Socket Layer is a protocol for transmitting private documents using the Internet. SSL works by using a public key to encrypt data that is transferred over the SSL connection. SSL uses the public-and-private key encryption system, which includes the use of a digital certificate. SSL is used for other applications than SSH, for example, OpenFlow.

STP

Spanning Tree Protocol, defined in IEEE 802.1d, used to eliminate redundant data paths and to increase network efficiency. STP allows a network to have a topology that contains physical loops; it operates in bridges and switches. STP opens certain paths to create a tree topology, thereby preventing packets from looping endlessly on the network. To establish path redundancy, STP creates a tree that spans all of the switches in an extended network, forcing redundant paths into a standby, or blocked, state.

STP allows only one active path at a time between any two network devices (this prevents the loops) but establishes the redundant links as a backup if the initial link should fail. If STP costs change, or if one network segment in the STP becomes unreachable, the spanning tree algorithm reconfigures the STP topology and re-establishes the link by activating the standby path.

syslog

A protocol used for the transmission of event notification messages across networks, originally developed on the University of California Berkeley Software Distribution (BSD) TCP/IP system implementations, and now embedded in many other operating systems and networked devices. A device generates a messages, a relay receives and forwards the messages, and a collector (a syslog server) receives the messages without relaying them.
syslog uses the UDP as its underlying transport layer mechanism. The UDP port that has been assigned to syslog is 514. (RFC 3164)

virtual router

In the Extreme Networks implementations, virtual routers allow a single physical switch to be split into multiple virtual routers. Each virtual router has its own IP address and maintains a separate logical forwarding table. Each virtual router also serves as a configuration domain. The identity of the virtual router you are working in currently displays in the prompt line of the CLI. The virtual routers discussed in relation to Extreme Networks switches themselves are not the same as the virtual router in VRRP.

In VRRP, the virtual router is identified by a virtual router (VRID) and an IP address. A router running VRRP can participate in one or more virtual routers. The VRRP virtual router spans more than one physical router, which allows multiple routers to provide redundant services to users.