Sun Netra™ CP3240 Switch Software Reference Manual

Sun Microsystems, Inc.
www.sun.com

Part No. 820-3253-12
January 2010, Revision A

Submit comments about this document at: `http://www.sun.com/hwdocs/feedback`

Contents

6. IP Multicast Commands 319

Figures

Tables

Preface

The *Sun Netra CP3240 Switch Software Reference Manual* describes the FASTPATH software used with the Sun Netra CP3240 switch boards for the Sun Netra™ CT 900 server and other compatible ATCA chassis.

The intended reader of this manual is an experienced system administrator who has experience with switches and routing. The reader should be comfortable with LAN fundamentals and with networking in general.

Before You Read This Book

Review the information in the *Sun Netra CP3x40 Switch Safety and Compliance Manual* before proceeding with the instructions in this document. The *Sun Netra CP3x40 Switch Safety and Compliance Manual* specifies the environmental and electrical safety requirements for the product and contains compliance certification for various countries.

How This Book Is Organized

Chapter 1 gives an overview of the FASTPATH software.

Chapter 2 describes the command-line interface (CLI) syntax, conventions, and terminology.

Chapter 3 describes the Switching commands.

Chapter 4 describes the Routing commands

Chapter 5 decsribes the IPv6 commands.

Chapter 6 describes the IP Multicast commands.

Chapter 7 describes the Quality of Service (QoS) commands.

Chapter 8 describes the utility commands.

Chapter 9 describes the management commands.

Typographic Conventions

Typeface[*]	Meaning	Examples
`AaBbCc123`	The names of commands, files, and directories; on-screen computer output	Edit your `.login` file. Use `ls -a` to list all files. `% You have mail.`

`AaBbCc123`	What you type, when contrasted with on-screen computer output	`%` **`su`**
		`Password:`

AaBbCc123	Book titles, new words or terms, words to be emphasized. Replace command-line variables with real names or values.	Read Chapter 6 in the *User's Guide*. These are called *class* options. You *must* be superuser to do this. To delete a file, type `rm` *filename*.

[*] The settings on your browser might differ from these settings.

Related Documentation

The following table lists the documentation for this product. The online documentation is available at:

`http://docs.sun.com/app/docs/prod/cp3240.switch?l=en#hic`

Application	Title	Part Number	Format	Location
Latest information	*Sun Netra CP3x40 Switch Product Notes*	820-3260-*xx*	PDF	Online
Ponter doc	*Sun Netra CP3240 Switch Getting Started Guide*	820-3254-*xx*	Printed	Shipping Kit
Usage	*Sun Netra CP3240 Switch User's Guide*	820-3252-*xx*	PDF	Online
Reference	*Sun Netra CP3240 Switch Software Reference Manual*	820-3253-*xx*	PDF	Online
Safety	*Sun Netra CP3x40 Switch Safety and Compliance Manual*	820-3505-*xx*	PDF	Online

The following table lists the documentation that is related to this product. The online documentation is available at:

`http://docs.sun.com/app/docs/prod/n900.srvr#hic`

Application	Title	Part Number	Format	Location
Latest information	*Sun Netra CT 900 Server Product Notes*	819-1180-*xx*	PDF	Online
Pointer Doc	*Sun Netra CT 900 Server Getting Started Guide*	819-1173-*xx*	Printed	Shipping kit
Overview	*Sun Netra CT 900 Server Overview*	819-1174-*xx*	PDF	Online
Installation	*Sun Netra CT 900 Server Installation Guide*	819-1175-*xx*	PDF	Online
Service	*Sun Netra CT 900 Server Service Manual*	819-1176-*xx*	PDF	Online
Administration	*Sun Netra CT 900 Server Administration and Reference Manual*	819-1177-*xx*	PDF	Online
Programming	*Sun Netra CT 900 Software Developer's Guide*	819-1178-*xx*	PDF	Online
Safety	*Sun Netra CT 900 Server Safety and Compliance Guide*	819-1179-*xx*	PDF	Online
Setup	*Sun Netra CT 900 Server Hardware Setup Guide*	819-1647-*xx*	PDF	Online
Safety	*Important Safety Information for Sun Hardware Systems*	816-7190-*xx*	Printed	Shipping kit

Documentation, Support, and Training

Sun Function	URL	Description
Documentation	`http://www.sun.com/documentation/`	Download PDF and HTML documents, and order printed documents
Support and Training	`http://www.sun.com/supportraining/`	Obtain technical support, download patches, and learn about Sun courses

Third-Party Web Sites

Sun is not responsible for the availability of third-party web sites mentioned in this document. Sun does not endorse and is not responsible or liable for any content, advertising, products, or other materials that are available on or through such sites or resources. Sun will not be responsible or liable for any actual or alleged damage or loss caused by or in connection with the use of or reliance on any such content, goods, or services that are available on or through such sites or resources.

Sun Welcomes Your Comments

Sun is interested in improving its documentation and welcomes your comments and suggestions. You can submit your comments by going to:

`http://www.sun.com/hwdocs/feedback`

Please include the title and part number of your document with your feedback:

Sun Netra CP3240 Switch Software Reference Manual, part number 820-3253-12

CHAPTER 1

FASTPATH Software

The FASTPATH software has two purposes:

- To assist attached hardware in switching frames, based on layer 2, 3, or 4 information contained in the frames.
- To provide a complete device management portfolio to the network administrator.

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

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

- CPU: This code runs the networking device management portfolio and controls the overall networking device hardware. It also assists in frame forwarding, as needed and specified. This code is designed to run on multiple platforms with minimal changes from platform to platform.
- Networking device processor: This code does the majority of the packet switching, usually at wire speed. This code is platform dependent, and substantial changes might exist across products.

FASTPATH provides the network administrator with a set of comprehensive management functions for managing both FASTPATH and the network. The network administrator has a choice of these easy-to-use management methods:

- VT100 interface
- Simple Network Management Protocol (SNMP)

Note – When configuring a device by use of a configuration file, the maximum number of configuration file command lines is 2000.

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

This chapter includes the following topics:

- "FASTPATH On the Sun Netra CP3240 Switch" on page 2
  - "Sun Netra CP3240 Defaults" on page 2
  - "Protocol, RFC, and MIB Support" on page 3

FASTPATH On the Sun Netra CP3240 Switch

The FASTPATH software provides the following functionality:

- L2 switching with all the ports in VLAN 1
- SNMP management
- Telnet management
- Serial management

Sun Netra CP3240 Defaults

The Sun Netra CP3240 switches come configured with a default configuration. This configuration boots the board to Layer 2 switching. This configuration is very basic and should be updated for your environment. The default settings are:

- Switch is configured with all ports enabled, set to auto-negotiate, MTU of 1518, and MAC switching mode in layer 2
- All ports are in VLAN 1
- DHCP client is enabled on the Out-of-band management port.
- Telnet access enabled
- SNMP read only community "public"
- SNMP read write community "private"

Note – SNMPv3 traps are not supported on the Sun Netra CP3240 switches.

The Spanning Tree Protocol (STP) and Secure Shell (SSH) are not enabled in the default configuration.

Note – The Sun Netra CP3240 switch supports SSH for a secure CLI console but cannot generate its own keys. Keys must be generated on an external PC and uploaded to the Sun Netra CP3240 via TFTP. Once the keys are on the Sun Netra CP3240, SSH must be enabled to be used.

Protocol, RFC, and MIB Support

FASTPATH software provides support for the following protocols, RFCs, and MIBs.

Switching

- IEEE 802.3ac - VLAN Tagging
- IEEE 802.3ad - Link Aggregation
- IEEE 802.1S - Multiple Spanning Tree (MSTP)
- IEEE 802.1W - Rapid Spanning Tree (RSTP)
- IEEE 802.1D - Spanning Tree (STP)
- GARP - Generic Attribute Registration Protocol
- GMRP - Dynamic L2 Multicast Registration
- GVRP - Dynamic VLAN Registration
- IEEE 802.1Q - Virtual LANs with Port based VLANs
- IEEE 802.1v - Protocol-based VLANs
- IEEE 802.1p - Ethernet Priority with User Provisioning & Mapping
- IEEE 802.1X - Port Based Authentication
- IEEE 802.3x - Flow Control

Advanced Layer 2 Functionality

- Broadcast Storm Recovery
- Double VLAN/vMAN Tagging (Q-in-Q)
- IGMP Snooping
- Independent VLAN Learning (IVL) support
- IPv6 Classification APIs
- Jumbo Ethernet Frames
- Port Mirroring
- Static MAC Filtering

System Facilities

- Event and Error Logging Facility
- Run-time and Configuration Download Capability
- PING Utility
- XMODEM, YMODEM, & ZMODEM
- RFC 768 - UDP
- RFC 783 - TFTP
- RFC 791 - IP
- RFC 792 - ICMP
- RFC 793 - TCP
- RFC 826 - ARP
- RFC 951 - BootP
- RFC 1321 - Message Digest Algorithm
- RFC 1534 - Interoperation between BootP and DHCP
- RFC 2131 - DHCP Client/Server
- RFC 2132 - DHCP Options and BootP Vendor Extensions
- RFC 2865 - RADIUS Client
- RFC 2866 - RADIUS Accounting
- RFC 2868 - RADIUS Attributes for Tunnel Protocol
- RFC 2869 - RADIUS Extensions
- RFC2869bis- RADIUS Support for Extensible Authentication Protocol (EAP)
- RFC 3580 - 802.1X RADIUS Usage Guidelines

Switching MIBs

- RFC 1213 - MIB-II
- RFC 1493 - Bridge MIB
- RFC 1643 - Ethernet-like MIB
- RFC 2674 - VLAN MIB
- RFC 2618 - RADIUS Authentication Client MIB
- RFC 2620 - RADIUS Accounting MIB
- RFC 2737 - Entity MIB version 2
- RFC 2819 - RMON Groups 1,2,3, & 9
- IEEE 802.1X (IEEE 802.1-PAE-MIB)
- FASTPATH Enterprise MIB

Routing

- RFC 826 - Ethernet ARP
- RFC 894 - Transmission of IP Datagrams over Ethernet Networks
- RFC 896 - Congestion Control in IP/TCP Networks
- RFC 1058 - RIP v1
- RFC 1256 - ICMP Router Discovery Messages
- RFC 1321 - Message Digest Algorithm
- RFC 1519 - CIDR
- RFC 1583 - OSPF v2
- RFC 1723 - RIP v2
- RFC 1765 - OSPF Database Overview
- RFC 1812 - Requirements for IP Version 4 Routers
- RFC 2082 - RIP-2 MD5 Authentication
- RFC 2328 - OSPF v2 w/ Equal Cost Multipath
- RFC 2338 - VRRP
- RFC 2453 - RIP v2
- RFC 3046 - DHCP/BootP Relay
- RFC 3101 - OSPF “Not So Stubby Area” (NSSA) Option Route Redistribution across RIP, OSPF, and BGP

Routing MIBS

- RFC 1724 - RIP v2 MIB Extension
- RFC 1850 - OSPF MIB
- RFC 2233 - The Interfaces Group MIN using SMI v2
- RFC 2787 - VRRP MIB

Quality of Service (QOS)

Differentiated Services (DiffServ)

- RFC 2474 - Definition of Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers
- RFC 2475 - An Architecture for Differentiated Services
- RFC 2597 - Assured Forwarding PHB Group
- RFC 3246 – An Expedited Forwarding PHB (Per-Hop Behavior)
- RFC 3260 – New Terminology and Clarifications for DiffServ

Access Control List (ACLs)

Permit/Deny actions for Inbound or Outbound traffic classification based on:

- Type of Service (ToS) or Differentiated Services DSCP
- Source IP Address
- Destination IP Address
- TCP/UDP Source Port
- TCP/UDP Destination Port
- IP Protocol Number

QoS MIBS

- RFC 3289 – Management Information Base for the Differentiated Services Architecture
- MIBs for full configuration of DiffServ, ACL and Bandwidth Provisioning functionality

Management

- RFC 854 – Telnet
- RFC 855 – Telnet Option
- RFC 1155 – SMI v1
- RFC 1157 – SNMP
- RFC 1212 – Concise MIB Definitions
- RFC 1867 – HTML/2.0 Forms with file upload extensions
- RFC 1901 – Community based SNMP v2
- RFC 1905 – Protocol Operations for SNMP v2
- RFC 1906 – Transport Mappings for SNMP v2
- RFC 1907 – Management Information Base for SNMP v2
- RFC 1908 – Coexistence between SNMP v1 and SNMP v2
- RFC 2068 – HTTP/1.1 protocol as updated by draft-ietf-http-v11-rev-03
- RFC 2271 – SNMP Framework MIB
- RFC 2295 – Transparent Content Negotiation
- RFC 2296 – Remote Variant Selection; RSVA/1.0 State Management "cookies" – draft-ietf-http-state-mgmt-05
- RFC 2570 – Introduction to SNMP v3
- RFC 2571 – Architecture for Describing SNMP Management Frameworks
- RFC 2572 – Message Processing and Dispatching for SNMP
- RFC 2573 – SNMP v3 Applications
- RFC 2574 – User Based Security Model for SNMP v3
- RFC 2575 – View based Access Control Model for SNMP
- RFC 2576 0 Coexistence between SNMP v1, V2, and v3
- RFC 2578 – SMI v2
- RFC 2579 – Textual Conventions for SMI v2
- RFC 2580 – Conformance statements for SMI v2 Configurable Management VLAN
- SSL 3.0 and TLS 1.0
- RFC 2246 - The TLS Protocol, Version 1.0
- RFC 2818 – HTTP over TLS
- RFC 2346 – AES Ciphersuites for Transport Layer Security
- SSH 1.5 and 2.0
- Draft-ietf-secsh-transport-16 – SSH Transport Layer Protocol
- Draft-ietf-secsh-userauth-17 – SSH Authentication Protocol

- Draft-ietf-secsh-connect-14 – SSH Protocol Architecture
- Draft-ietf-secsh-publickeyfile-03 – SECSH Public Key File Format
- Draft-ietf-sech-dh-group-exhange-04 – Diffie-Hellman Group Exchange for the SSH Transport Layer Protocol
- HTML 4.0 Specification – December, 1997
- Java and Java Script 1.3

Other

- Industry standard CLI
    - scripting capability
    - command completion
    - context sensitive help
- User password encryption
- Multi-session Telnet Server

CHAPTER 2

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. It contains the following sections:

Command Syntax

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

Some commands, such as `show network` or `clear vlan`, do not require parameters. Other commands, such as `network parms`, have parameters for which you must supply a value. Parameters are positional—you must type the values in the correct order. Optional parameters will follow required parameters. Following are two examples.

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

In the preceding example, <ipaddr> and <netmask> are the required values for the command, and [gateway] is the optional value for the command.

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

In the second example, <loc> is the required parameter for the command.

Command Conventions

The following conventions apply to the command name:

- The command name is displayed in this document in monospace font and must be typed exactly as shown.
- Once you have entered enough letters of a command name to uniquely identify the command, pressing the spacebar or Tab key causes the system to complete the word.
- Pressing Ctrl-Z returns you to the root-level command prompt.

This reference manual lists each command by the command name and provides a brief description of the command. Each command entry contains the following information:

- Format shows the command keywords and parameters (required and optional).
- 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.

Parameter Conventions

The following conventions apply to parameters:

- Parameters are order dependent.
- Variables are displayed in this document in italic font, and must be replaced with a name or number.
- To use spaces as part of a name parameter, enclose it 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.
- Parameters might be mandatory values, optional values, choices, or a combination. Parameter values might be names (strings) or numbers.

Table 2-1 describes the conventions this document uses to distinguish between value types.

TABLE 2-1 Parameter Value Types

Symbol	**Example**	**Description**
<> angle brackets	*`<value>`*	Indicates that you must enter a value in place of the brackets and text inside them.
[] square brackets	*`[value]`*	Indicates an optional parameter that you can enter in place of the brackets and text inside them.
{} 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.

Parameter Values

The following conventions apply to the values of the common parameters. Table 2-2 describes common parameter values and formatting.

TABLE 2-2 Common Parameter Values

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, hexidecimal and octal formats through the following input formats (where *n* is any valid hexidecimal, octal or decimal number): • 0x*n* (CLI assumes hexidecimal format) • 0*n* (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.
areaid	Enter area IDs in dotted-decimal notation (for example, 0.0.0.1). • An area ID of 0.0.0.0 is reserved for the backbone. • Area IDs have the same format as IP addresses but are distinct from IP addresses. • You can use the IP network number of the sub-netted network for the area ID.
routerid	Enter the value of `<routerid>` in dotted-decimal notation, such as 0.0.0.1. A router ID of 0.0.0.0 is invalid.
Interface or slot/port	Valid slot and port number separated by forward slashes. For example, 0/1 represents slot number 0 and port number 1.
Logical Interface	Represents a Logical slot and port number.. This is applicable in the case of a port-channel (LAG). You can use the logical slot/port to configure the port-channel.
Character strings	Use double quotation marks to identify character strings, for example, “System Name with Spaces.” An empty string (“”) is not valid.

Slot/Port Naming Convention

FASTPATH software references physical entities such as cards and ports by using a slot/port naming convention. The FASTPATH software also uses this convention to identify certain logical entities, such as 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 2-3 Slot Types

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

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

TABLE 2-4 Port Types

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

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

“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.

The behavior of the “?” and the help text are the same for the `no` keyword:

- The help message is the same for all forms of the command. The help string might be augmented with details about the `no` form behavior.
- For the (`no interface?`) and (`no inte?`) cases, the help options displayed are identical to the case when the `no` token is not specified, as in (`interface?`) and (`inte?`).

Command Modes

The CLI groups commands into modes according to the command function. Each of the command modes supports specific FASTPATH software commands. The commands in one mode are not available until you switch to that particular mode, 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 2-5 lists the command modes, the prompts visible in each mode, and the exit method from that mode.

Topology is described in See “Mode-Based Topology” on page 17..

Descriptions and hierarchy of each mode are in See “Mode-Based Command Hierarchy” on page 19..

TABLE 2-5 CLI Command Modes

Command Mode	Access Method	Prompt	Exit or Access Previous Mode
User Exec	This is the first level of access for performing basic tasks and listing system information.	`Switch>`	Enter `logout` command
Privileged Exec	From the User Exec mode, enter the `enable` command.	`Switch#`	Type `exit` or press `Ctrl-Z` to exit to the User Exec mode.
Global Config	From the Privileged Exec mode, enter the `configure` command.	`Switch(Config)#`	Type `exit` to exit to the Privileged Exec mode, or press `Ctrl-Z` to switch to the User Exec mode.
VLAN Config	From the Privileged Exec mode, enter the `vlan database` command.	`Switch(Vlan)#`	Type `exit` to exit to the Privileged Exec mode, or press `Ctrl-Z` to switch to the User Exec mode.

Interface Config	From the Global Config mode, enter the `interface` <slot/port> command.	`Switch (Interface <`*`slot/port`*`>)#`
		`Switch (Interface Loopback <`*`id`*`>)#`
		`Switch (Interface Tunnel <`*`id`*`>)#`
			Type `exit` to exit to the Global Config mode, or press `Ctrl-Z` to switch to the User Exec mode.

Line Config	From the Global Config mode, enter the `lineconfig` command.	`Switch (line)#`	Type `exit` to exit to the Global Config mode, or press `Ctrl-Z` to switch to the User Exec mode.
Policy Map Config	From the Global Config mode, enter the `policy-map <policy-name>` command.	`Switch (Config-policy-map)#`	Type `exit` to exit to the Global Config mode, or press `Ctrl-Z` to switch to the User Exec mode.
Policy Class Config	From the Policy Map mode, enter the `class` command.	`Switch (Config-policy-class-map)#`	Type `exit` to exit to the Policy Map mode, or press `Ctrl-Z` to switch to the User Exec mode.
Class Map Config	From the Global Config mode, enter the `class-map <class-map-name>` command.	`Switch (Config-class-map)#`	Type `exit` to exit to the Global Config mode, or press `Ctrl-Z` to switch to the User Exec mode.

TABLE 2-5 CLI Command Modes *(Continued)*

Command Mode	**Access Method**	**Prompt**	**Exit or Access Previous Mode**
Router OSPF Config	From the Global Config mode, enter the `router ospf` command.	`Switch (Config-router)#`	Type `exit` to exit to the Global Config mode, or press `Ctrl-Z` to switch to the User Exec mode.
Router OSPFv3 Config	From the Global Config mode, enter the `ipv6 router ospf` command.	`Switch (Config-rtr)#`	Type `exit` to exit to the Global Config mode, or press `Ctrl-Z` to switch to the User Exec mode.
Router RIP Config	From the Global Config mode, enter the `router rip` command.	`Switch (Config-router)#`	Type `exit` to exit to the Global Config mode, or press `Ctrl-Z` to switch to the User Exec mode.
Router BGP Config	From the Global Config mode, enter the `router bgp` <*asnumber*> command.	`Switch (Config-router)#`	Type `exit` to exit to the Global Config mode, or press `Ctrl-Z` to switch to the User Exec mode.
MAC Access-list Config	From the Global Config mode, enter `mac access-list extended` <*name*>.	`Switch (Config-mac-access-list)#`	Type `exit` to exit to the Global Config mode, or press `Ctrl-Z` to switch to the Privileged EXEC mode.
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.	`Switch (Tacacs)#`	Type `exit` to exit to the Global Config mode, or press `Ctrl-Z` to switch to the Privileged EXEC mode.
DHCP Pool Config	From the Global Config mode, enter the `ip dhcp pool` <pool-name> command.	`Switch (Config-dhcp-pool)#`	Type `exit` to exit to the Global Config mode, or press `Ctrl-Z` to switch to the Privileged EXEC mode.
DHCPv6 Pool Config	From the Global Config mode, enter the `ip dhcp pool` <pool-name> command.	`Switch (Config-dhcp6-pool)#`	Type `exit` to exit to the Global Config mode, or press `Ctrl-Z` to switch to the Privileged EXEC mode.

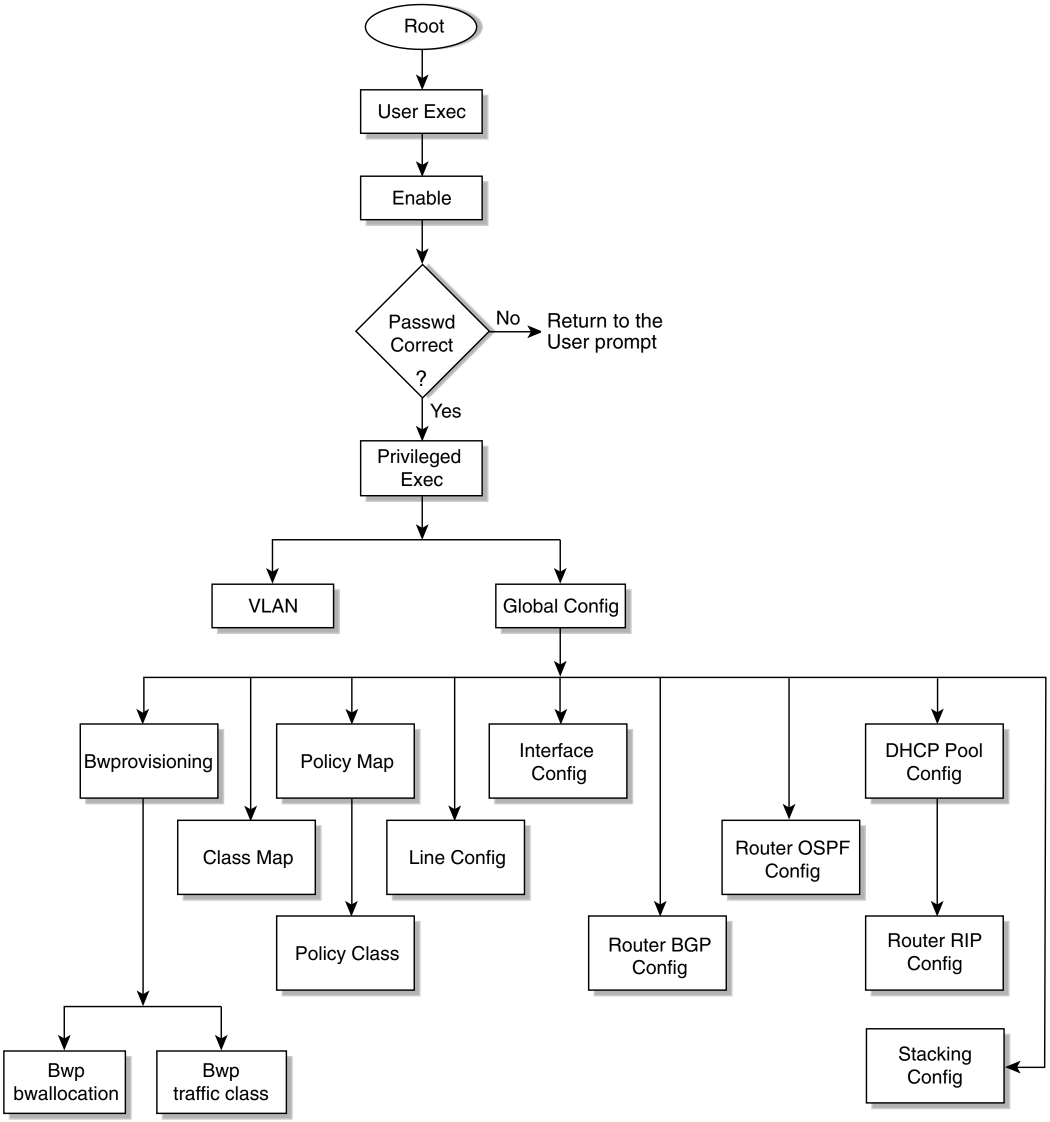
Mode-Based Topology

The CLI tree is built on a mode concept in which the commands are available according to the interface. Some of the modes in the mode-based CLI are depicted in FIGURE 2-1.

Note – The User Exec commands are also accessible in the Privileged Exec Mode.

Note – Access to all commands in the Privileged Exec mode and below is restricted through a password.

FIGURE 2-1 Mode-based CLI



Mode-Based Command Hierarchy

The commands in one mode are not available until the operator switches to that particular mode, with the exception of the User Exec mode commands. The User Exec mode commands can also be executed in the Privileged Exec mode.

The commands available to the operator at any time depend upon the mode. Entering a question mark (?) at the CLI prompt displays a list of the currently available commands and descriptions of the commands.

User Exec Mode

When the operator logs in to the CLI, the User Exec mode is the initial mode. The User Exec mode contains a limited set of commands. The command prompt shown at this level is `$ Switch>`

Privileged Exec Mode

To have access to the full suite of commands, the operator must enter the Privileged Exec mode. The Privileged Exec mode requires password authentication. From Privileged Exec mode, the operator can issue any Exec command, enter the VLAN mode or enter the Global Config mode. The command prompt shown at this level is `$ Switch#`

Global Config Mode

This mode permits the operator to make modifications to the running configuration. General setup commands are grouped in this mode. From the Global Config mode, the operator can enter the System Config mode, the Physical Port Config mode, the Interface Config mode, or the protocol-specific modes. The command prompt at this level is `$ Switch (Config)#`

From the Global Config mode, the operator can enter the following protocol-specific modes configuration modes.

Interface Config

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

This mode allows you to enable or modify the operation of an interface and provides access to the router interface configuration commands.

Use this mode to set up a physical port for a specific logical connection operation.

In this mode, a physical port is set up for a specific logical connection operation. The Interface Config mode provides access to the router interface configuration commands. The command prompt at this level is `$ Switch (Interface <slot/port>)#`

The resulting prompt for the interface configuration command entered in the Global Configuration mode is `$ Switch (Interface Loopback <`*`id`*`>` and `$ Switch (Interface Tunnel <`*`id`*`>`.

Line Config

This mode allows the operator to configure the console interface. The operator can configure the interface from the directly connected console or the virtual terminal used with Telnet. The command prompt at this level is `$ Switch(line)#`

Policy Map Config

Use the `policy-map` <policy-name> command to access the QoS policy map configuration mode to configure the QoS policy map.

```
$ Switch (Config)# policy map <policy-name>
```

```
$ Switch (Config-policy-map)#
```

Policy Class Config

Use the `class` <class-name> command to access the QoS policy-classmap mode to attach or remove a diffserv class to a policy and to configure the QoS policy class.

```
$ Switch (Config policy-map)# class <class-name>
```

```
$ Switch (Config-policy-classmap)#
```

Class Map Config

This mode consists of class creation, deletion, and matching commands. The class match commands specify layer 2, layer 3, and general match criteria. Use the `class-map` <class-map-name> commands to access the QoS class map configuration mode to configure QoS class maps.

```
$ Switch (Config)# class-map <class-map-name>
```

```
$ Switch (Config class-map)#
```

Router OSPF Config

In this mode, the operator is allowed to access the router OSPF configuration commands. The command prompt at this level is:

```
$ Switch (Config)# router ospf
```

```
$ Switch (Config-router) #
```

Router OSPFv3 Config

In this mode, the operator is allowed to access the router OSPFv3 configuration commands. The command prompt at this level is:

```
$ Switch (Config)# rtr ospf
```

```
$ Switch (Config-rtr) #
```

Router RIP Config

In this mode, the operator is allowed to access the router RIP configuration commands. The command prompt at this level is:

```
$ Switch (Config)# router rip
```

```
$ Switch (Config router)#
```

Router BGP Config

In this mode, the operator is allowed to access the router BGP-4 configuration commands. The command prompt at this level is:

```
$ Switch (Config)# router bgp <1-65535>
$ Switch (Config-routerbgp)#
```

MAC Access-list Config

In this mode, the operator is allowed to create a MAC Access-list and to enter the mode containing Mac Access-list configuration commands. The command prompt at this level is:

```
$ Switch (Config)# mac access-list extended <name>
```

```
$ Switch (Config-mac-access-list) #
```

TACACS Config

In this mode, the operator is allowed to configure properties for the TACACS servers. The command prompt at this level is:

```
$ Switch (Config)# tacacs-server host <ip-addr>
```

```
$ Switch (Tacacs) #
```

DHCP Pool Config

Use the `ip dhcp pool` <pool-name> command to access the DHCP Pool Config mode.

```
$ Switch (Config)# ip dhcp pool <pool-name>
```

```
$ Switch (Config-dhcp-pool)#
```

DHCPv6 Pool Config

Use the `ip dhcp pool` <pool-name> command to access the DHCP Pool Config mode.

```
$ Switch (Config)# ip dhcpv6 pool <pool-name>
```

```
$ Switch (Config-dhcp6-pool)#
```

VLAN Mode

This mode groups all the commands pertaining to VLANs. The command prompt shown at this level is `$ Switch (Vlan)#`

Operation Flow

This section captures the flow of operation for the CLI.

1. The operator logs in to the CLI session and enters the User Exec mode. In the User Exec mode, the `$(exec)>` prompt is displayed on the screen.

   The parsing process is initiated whenever the operator types a command and presses Enter. The command tree is searched for the command of interest. If the command is not found, the output message indicates where the offending entry begins. For instance, if command node A has the command `show arp brief` but the operator attempts to execute the command `show arpp brief`, the output message is `$(exec)> show arpp brief^. $%Invalid input detected at '^'` marker.

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

```
(exec) #show arpp brief
                ^
%Invalid input detected at '^' marker.
```

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

2. After the command is successfully parsed and validated, the control of execution goes to the corresponding CLI callback function.

3. For mandatory parameters, the command tree extends until the mandatory parameters make the leaf of the branch. The callback function is invoked only when all the mandatory parameters are provided. For optional parameters, the command tree extends until the mandatory parameters and the optional parameters make the leaf of the branch. However, the callback function is associated with the node where the mandatory parameters are fetched. The callback function then takes care of the optional parameters.

4. Once the control has reached the callback function, the callback function has complete information about the parameters entered by the operator.

Command Completion and Abbreviation

Command completion finishes spelling the command when you have typed enough letters of a command to uniquely identify the command word. You can execute the command by pressing the Enter key (command abbreviation) or you can complete the command word by pressing the Tab or spacebar keys (command completion).

The value "`Er`" designates that the requested value was not internally accessible. This should not happen and indicates that the software is not handling this instance correctly.

The value of "-----" designates that the value is unknown.

CLI Error Messages

If you enter a command and the system is unable to execute it, an error message appears. Table 2-6 describes the most common CLI error messages.

TABLE 2-6 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 2-7 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 2-7 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.

```
(switch) >?

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

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

```
(switch) #network ?

javamode                 Enable/Disable.
mgmt_vlan                Configure the Management VLAN ID of the
switch.
parms                  Configure Network Parameters of the router.
protocol               Select DHCP, BootP, or None as the network
config
                         protocol.
```

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

```
(switch) #network parms ?

<ipaddr>                 Enter the IP Address.
```

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

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

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

```
 (switch) #show m?

mac-addr-table              mac-address-table           monitor
```

Accessing the CLI

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

For the initial connection, you must use a direct connection to the console port. You cannot access the system remotely until the system has an IP address, subnet mask, and default gateway. You can set the network configuration information manually, or you can configure the system to accept these settings from a BOOTP or DHCP server on your network. For more information, see "Network Interface Commands" on page 478.

Comments

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

Some examples of comments are provided in the following code.

```
! Script file for displaying the ip interface
! Display information about interfaces
show ip interface 0/1 !Displays the information about the first interface
! Display information about the next interface
show ip interface 0/2
! End of the script file
```

CHAPTER 3

Switching Commands

This chapter describes the switching commands available in the FASTPATH® CLI.

The Switching Commands chapter includes the following sections:

Command Function Groups

This section provides a detailed explanation of the FASTPATH software platform commands. The commands are divided into three functional groups:

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

Port Configuration Commands

This section describes the commands you use to view and configure port settings.

interface

This command gives you access to the Interface Config mode, which allows you to enable or modify the operation of an interface (port).

Format	**`interface`** *`<slot/port>`*
Mode	Global Config

auto-negotiate

This command enables automatic negotiation on a port.

Default	enabled
Format	**`auto-negotiate`**
Mode	Interface Config

no auto-negotiate

This command disables automatic negotiation on a port.

Note – Automatic sensing is disabled when automatic negotiation is disabled.

Format	**`no auto-negotiate`**
Mode	Interface Config

auto-negotiate all

This command enables automatic negotiation on all ports.

Default	enabled
Format	**`auto-negotiate all`**
Mode	Global Config

no auto-negotiate all

This command disables automatic negotiation on all ports.

Format	**`no auto-negotiate all`**
Mode	Global Config

description

Use this command to create an alpha-numeric description of the port.

Format	**`description`** *<description>*
Mode	Interface Config

mtu

Use the **`mtu`** command to set the maximum transmission unit (MTU) size, in bytes, for frames that ingress or egress the interface. You can use the **`mtu`** command to configure jumbo frame support for physical and port-channel (LAG) interfaces. For the standard FASTPATH implementation, the MTU size is a valid integer between 1522 - 9216 for tagged packets and a valid integer between 1518 - 9216 for untagged packets.

Note – To receive and process packets, the Ethernet MTU must include any extra bytes that Layer-2 headers might require. To configure the IP MTU size, which is the maximum size of the IP packet (IP Header + IP payload), see "ip mtu" on page 174.

Default	1518 (untagged)
Format	**`mtu`** *`<1518-9216>`*
Mode	Interface Config

no mtu

This command sets the default MTU size (in bytes) for the interface.

Format	**`no mtu`**
Mode	Interface Config

pre-emphasis level

This command is used only on 10G CX4 interfaces. This command manually adjusts pre-emphasis for varying cable lengths. In general, higher values are for longer cable lengths.

Default	10
Format	**`pre-emphasis level`** *`<1-15>`*
Mode	Interface Config, Sun Netra CP3240 switch only

shutdown

This command disables a port.

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`

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

Format	**`speed`** *`{<100	10> <half-duplex	full-duplex>}`*
Mode	Interface Config

Acceptable values are:

100h	100BASE-T half duplex
100f	100BASE-T full duplex
10h	10BASE-T half duplex
10f	10BASE-T full duplex

`speed all`

This command sets the speed and duplex setting for all interfaces.

Format	**`speed all`** *`{<100	10> <half-duplex	full-duplex>}`*
Mode	Global Config

Acceptable values are:

100h	100BASE-T half-duplex
100f	100BASE-T full duplex
10h	10BASE-T half duplex
10f	10BASE-T full duplex

show port

This command displays port information.

Format	**`show port`** *`{<slot/port>	all}`*
Mode	Privileged EXEC

Interface	Valid slot and port number separated by forward slashes.
Type	If not blank, this field indicates that this port is a special type of port. The possible values are as follows: • **Mirror** - this port is a monitoring port. For more information, see "Port Mirroring" on page 117. • **PC Mbr**- this port is a member of a port-channel (LAG). • **Probe** - this port is a probe port.
Admin Mode	Selects 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	Selects 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	Indicates the port speed and duplex mode.
Link Status	Indicates whether the Link is up or down.
Link Trap	This object determines whether or not to send a trap when link status changes. The factory default is enabled.
LACP Mode	Displays whether LACP is enabled or disabled on this port.

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

Group Name	Displays the group name of an entry in the Protocol-based VLAN table.
Group ID	Displays the group identifier of the protocol group.
Protocol(s)	Indicates the type of protocol(s) for this group.
VLAN	Indicates the VLAN associated with this Protocol Group.
Interface(s)	Lists the slot/port interface(s) that are associated with this Protocol Group.

Spanning Tree Protocol (STP) Commands

This section describes the commands you use to configure Spanning Tree Protocol (STP). STP helps prevent network loops, duplicate messages, and network instability.

Note – STP is disabled by default. When you enable STP on the switch, STP is still disabled on each port.

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	disabled
Format	**`spanning-tree`**
Mode	Global Config

no spanning-tree

This command sets the spanning-tree operational mode to disabled. While disabled, the spanning-tree configuration is retained and can be changed, but is not activated.

Format	**`no spanning-tree`**
Mode	Global Config

spanning-tree bpdumigrationcheck

Use this command to force a transmission of rapid spanning tree (RSTP) and multiple spanning tree (MSTP) BPDUs. Use the *`<slot/port>`* parameter to transmit a BPDU from a specified interface, or use the *`all`* keyword to transmit BPDUs from all interfaces. This command forces the BPDU transmission when you execute it, so the command does not change the system configuration or have a “no” version.

Format	**`spanning-tree bpdumigrationcheck`** *`{<slot/port> | all}`*
Mode	Global Config

spanning-tree configuration name

This command sets the Configuration Identifier Name for use in identifying the configuration that this switch is currently using. The *`<name>`* is a string of up to 32 characters.

Default	base MAC address in hexadecimal notation
Format	**`spanning-tree configuration name`** *`<name>`*
Mode	Global Config

no spanning-tree configuration name

This command resets the Configuration Identifier Name to its default.

Format	**`no spanning-tree configuration name`**
Mode	Global Config

spanning-tree configuration revision

This command sets the Configuration Identifier Revision Level for use in identifying the configuration that this switch is currently using. The Configuration Identifier Revision Level is a number in the range of 0 to 65535.

Default	0
Format	**`spanning-tree configuration revision`** *<0-65535>*
Mode	Global Config

no spanning-tree configuration revision

This command sets the Configuration Identifier Revision Level for use in identifying the configuration that this switch is currently using to the default value, 0.

Format	**no spanning-tree configuration revision**
Mode	Global Config

spanning-tree edgeport

This command specifies that this port is an Edge Port within the common and internal spanning tree. This will allow this port to transition to Forwarding State without delay.

Format	**spanning-tree edgeport**
Mode	Interface Config

no spanning-tree edgeport

This command specifies that this port is not an Edge Port within the common and internal spanning tree.

Format	**no spanning-tree edgeport**
Mode	Interface Config

spanning-tree forceversion

This command sets the Force Protocol Version parameter to a new value. The Force Protocol Version can be one of the following:

- 802.1d - ST BPDUs are transmitted rather than MST BPDUs (IEEE 802.1d functionality supported)
- 802.1w - RST BPDUs are transmitted rather than MST BPDUs (IEEE 802.1w functionality supported)
- 802.1s - MST BPDUs are transmitted (IEEE 802.1s functionality supported)

Following are the format and mode for the `spanning-tree forceversion` command.

Default	802.1s
Format	**`spanning-tree forceversion`** *`<802.1d	802.1s	802.1w>`*
Mode	Global Config

no spanning-tree forceversion

This command sets the Force Protocol Version parameter to the default value, 802.1s.

Format	**no spanning-tree forceversion**
Mode	Global Config

spanning-tree forward-time

This command sets the Bridge Forward Delay parameter to a new value for the common and internal spanning tree. The forward-time value is in seconds within a range of 4 to 30, with the value being greater than or equal to "(Bridge Max Age / 2) + 1".

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, 15.

Format	**no spanning-tree forward-time**
Mode	Global Config

spanning-tree hello-time

This command sets the Admin Hello Time parameter to a new value for the common and internal spanning tree. The hellotime <value> is in whole seconds within a range of 1 to 10 with the value being less than or equal to "(Bridge Max Age / 2) - 1".

Default	2
Format	**spanning-tree hello-time** *<1-10>*
Mode	Interface Config

no spanning-tree hello-time

This command sets the admin Hello Time parameter for the common and internal spanning tree to the default value.

Format	**no spanning-tree hello-time**
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 times - (Bridge Forward Delay - 1)".

Default	20
Format	**`spanning-tree max-age`** *`<6-40>`*
Mode	Global Config

no spanning-tree max-age

This command sets the Bridge Max Age parameter for the common and internal spanning tree to the default value, 20.

Format	**no spanning-tree max-age**
Mode	Global Config

spanning-tree max-hops

This command sets the MSTP Max Hops parameter to a new value for the common and internal spanning tree. The max-hops value is a range from 1 to 127.

Default	20
Format	**`spanning-tree max-hops`** *`<1-127>`*
Mode	Global Config

no spanning-tree max-hops

This command sets the Bridge Max Hops parameter for the common and internal spanning tree to the default value.

Format	**`no spanning-tree max-hops`**
Mode	Global Config

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 **external-cost** option, this command sets the external-path cost for MST instance ‘0’ i.e. CIST instance. You can set the external cost as a number in the range of 1 to 200000000 or **auto**. If you specify auto, the external 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 external-cost—auto port-priority—128
Format	**`spanning-tree mst`** *`<mstid> {{cost <1-200000000>	auto}	{external-cost <1-200000000>	auto}	port-priority <0-240>}`*
Mode	Interface Config

no spanning-tree mst

This command sets the Path Cost or Port Priority for this port within the multiple spanning tree instance, or in the common and internal spanning tree to the respective default values. If you specify an *<mstid>* parameter that corresponds to an existing multiple spanning tree instance, you are configuring that multiple spanning tree instance. If you specify 0 (defined as the default CIST ID) as the *<mstid>*, you are configuring the common and internal spanning tree instance.

If the you specify **cost**, this command sets the path cost for this port within a multiple spanning tree instance or the common and internal spanning tree instance, depending on the *<mstid>* parameter, to the default value, i.e. a path cost value based on the Link Speed.

If you specify **external-cost**, this command sets the external path cost for this port for mst '0' instance, to the default value, i.e. a path cost value based on the Link Speed.

If you specify **port-priority**, this command sets the priority for this port within a specific multiple spanning tree instance or the common and internal spanning tree instance, depending on the *<mstid>* parameter, to the default value.

Format	**no spanning-tree mst** *<mstid> <cost | external-cost | port-priority>*
Mode	Interface Config

spanning-tree mst instance

This command adds a multiple spanning tree instance to the switch. The instance <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 FASTPATH 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 instance <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 61440 in increments of 4096.

If you specify 0 (defined as the default CIST ID) as the *`<mstid>`*, this command sets the Bridge Priority parameter to a new value for the common and internal spanning tree. The bridge priority value is a number within a range of 0 to 61440. The twelve least significant bits are masked according to the 802.1s specification. This causes the priority to be rounded down to the next lower valid priority.

Default	32768
Format	**`spanning-tree mst priority`** *`<mstid> <0-61440>`*
Mode	Global Config

no spanning-tree mst priority

This command sets the bridge priority for a specific multiple spanning tree instance to the default value. 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	**spanning-tree mst priority** *<mstid>*
Mode	Global Config

spanning-tree mst vlan

This command adds an association between a multiple spanning tree instance and a VLAN so that the VLAN is no longer associated with the common and internal spanning tree. The parameter *<mstid>* is a number that corresponds to the desired existing multiple spanning tree instance. The *<vlanid>* corresponds to an existing VLAN ID.

Format	**`spanning-tree mst vlan`** *`<mstid> <vlanid>`*
Mode	Global Config

no spanning-tree mst vlan

This command removes an association between a multiple spanning tree instance and a VLAN so that the VLAN is again be associated with the common and internal spanning tree. The parameter *<mstid>* is a number that corresponds to the desired existing multiple spanning tree instance. The *<vlanid>* corresponds to an existing VLAN ID.

Format	**`no spanning-tree mst vlan`** *`<mstid> <vlanid>`*
Mode	Global Config

no spanning-tree port mode

This command sets the Administrative Switch Port State for this port to disabled.

Format	**no spanning-tree port mode**
Mode	Interface Config

spanning-tree port mode all

This command sets the Administrative Switch Port State for all ports to enabled.

Default	disabled
Format	**spanning-tree port mode all**
Mode	Global Config

no spanning-tree port mode all

This command sets the Administrative Switch Port State for all ports to disabled.

Format	**no spanning-tree port mode all**
Mode	Global Config

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`**
Modes	Privileged EXEC User EXEC

TABLE 0-1 Entry Definitions for `show spanning-tree` Without `brief` Parameter

Entry	Definition
Bridge Priority	Specifies the bridge priority for the Common and Internal Spanning tree (CST). The value lies between 0 and 61440. It is displayed in multiples of 4096.
Bridge Identifier	The bridge identifier for the CST. It is made up using the bridge priority and the base MAC address of the bridge.
Time Since Topology Change	Time in seconds.
Topology Change Count	Number of times changed.

TABLE 0-1 Entry Definitions for `show spanning-tree` Without `brief` Parameter

Entry	**Definition**
Bridge Priority	Specifies the bridge priority for the Common and Internal Spanning tree (CST). The value lies between 0 and 61440. It is displayed in multiples of 4096.
Topology Change	Boolean value of the Topology Change parameter for the switch indicating if a topology change is in progress on any port assigned to the common and internal spanning tree.
Designated Root	The bridge identifier of the root bridge. It is made up from the bridge priority and the base MAC address of the bridge.
Root Path Cost	Value of the Root Path Cost parameter for the common and internal spanning tree.
Root Port Identifier	Identifier of the port to access the Designated Root for the CST.
Root Port Max Age	Derived value.
Root Port Bridge Forward Delay	Derived value.
Hello Time	Configured value of the parameter for the CST.
Bridge Hold Time	Minimum time between transmission of Configuration Bridge Protocol Data Units (BPDUs)
Bridge Max Hops	Bridge max-hops count for the device.
CST Regional Root	Bridge Identifier of the CST Regional Root. It is made up using the bridge priority and the base MAC address of the bridge.
Regional Root Path Cost	Path Cost to the CST Regional Root.
Associated FIDs	List of forwarding database identifiers currently associated with this instance.
Associated VLANs	List of VLAN IDs currently associated with this instance.

`show spanning-tree brief`

When the “brief” optional parameter is included, this command displays spanning tree settings for the bridge.

Format	**`show spanning-tree brief`**
Modes	Privileged EXEC User EXEC

This command displays spanning tree settings for the bridge. The following information appears.

TABLE 0-2 Entry Definitions for `show spanning-tree` With `brief` Parameter

Bridge Priority	**Configured Value**
Bridge Identifier	The bridge identifier for the selected MST instance. It is made up using the bridge priority and the base MAC address of the bridge.
Bridge Max Age	Configured value.
Bridge Max Hops	Bridge max-hops count for the device.
Bridge Hello Time	Configured value.
Bridge Forward Delay	Configured value.
Bridge Hold Time	Minimum time between transmission of Configuration Bridge Protocol Data Units (BPDUs)

`show spanning-tree interface`

This command displays the settings and parameters for a specific switch port within the common and internal spanning tree. The *`<slot/port>`* is the desired switch port. The following details are displayed on execution of the command.

Format	**`show spanning-tree interface`** *`<slot/port>`*
Modes	Privileged EXEC User EXEC

TABLE 3-1 Entry Definitions for `show spanning-tree interface`

Entry	Definition
Hello Time	Admin hello time for this port.
Port Mode	Enabled or disabled.
Port Up Time Since Counters Last Cleared	Time since port was reset, displayed in days, hours, minutes, and seconds.
STP BPDUs Transmitted	Spanning Tree Protocol Bridge Protocol Data Units sent
STP BPDUs Received	Spanning Tree Protocol Bridge Protocol Data Units received.
RST BPDUs Transmitted	Rapid Spanning Tree Protocol Bridge Protocol Data Units sent
RST BPDUs Received	Rapid Spanning Tree Protocol Bridge Protocol Data Units received.
MSTP BPDUs Transmitted	Multiple Spanning Tree Protocol Bridge Protocol Data Units sent
MSTP BPDUs Received	Multiple Spanning Tree Protocol Bridge Protocol Data Units received.

show spanning-tree mst port detailed

This command displays the detailed settings and parameters for a specific switch port within a particular multiple spanning tree instance. The parameter *<mstid>* is a number that corresponds to the desired existing multiple spanning tree instance. The *<slot/port>* is the desired switch port.

Format	**`show spanning-tree mst port detailed`** *`<mstid>`*
	`<slot/port>`

Mode	Privileged EXEC User EXEC

TABLE 3-2 Entry Definitions for `show spanning-tree mst port detailed`

Entry	Definition
MST Instance ID	The ID of the existing MST instance.
Port Identifier	The port identifier for the specified port within the selected MST instance. It is made up 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
Auto-Calculate Port Path Cost	This indicates whether auto calculation for port path cost is enabled.
Port Path Cost	Configured value of the Internal Port Path Cost parameter.
Auto-Calculate External Port Path Cost	This indicates whether auto calculation for external port path cost is enabled.
External Port Path Cost	Configured value of the external Port Path Cost parameter.
Designated Root	The Identifier of the designated root for this port.
Designated Port Cost	Path Cost offered to the LAN by the Designated Port
Designated Bridge	Bridge Identifier of the bridge with the Designated Port.
Designated Port Identifier	Port on the Designated Bridge that offers the lowest cost to the LAN.

If you specify 0 (defined as the default CIST ID) as the *<mstid>*, this command displays the settings and parameters for a specific switch port within the common and internal spanning tree. The *<slot/port>* is the desired switch port. In this case, the following are displayed.

TABLE 3-3 Entry Definitions for `show spanning-tree mst port detailed` if `0` is Passed as the `<mtsid>`

Entry	**Definition**
Port Identifier	The port identifier for this port within the CST.
Port Priority	The priority of the port within the CST.
Port Forwarding State	The forwarding state of the port within the CST.
Port Role	The role of the specified interface within the CST.
Port Path Cost	The configured path cost for the specified interface.
Designated Root	Identifier of the designated root for this port within the CST.
Designated Port Cost	Path Cost offered to the LAN by the Designated Port.
Designated Bridge	The bridge containing the designated port
Designated Port Identifier	Port on the Designated Bridge that offers the lowest cost to the LAN
Topology Change Acknowledgement	Value of flag in next Configuration Bridge Protocol Data Unit (BPDU) transmission indicating if a topology change is in progress for this port.
Hello Time	The hello time in use for this port.
Edge Port	The configured value indicating if this port is an edge port.
Edge Port Status	The derived value of the edge port status. True if operating as an edge port; false otherwise.
Point To Point MAC Status	Derived value indicating if this port is part of a point to point link.
CST Regional Root	The regional root identifier in use for this port.
CST Port Cost	The configured path cost for this port.

`show spanning-tree mst port summary`

This command displays the settings of one or all ports within the specified multiple spanning tree instance. The parameter *`<mstid>`* indicates a particular MST instance. The parameter {*`<slot/port>`* `|` *`all`*} indicates the desired switch port or all ports.

If you specify 0 (defined as the default CIST ID) as the *<mstid>*, the status summary displays for one or all ports within the common and internal spanning tree.

Format	**`show spanning-tree mst port summary`** *`<mstid>`* *`{<slot/port>	all}`*
Modes	Privileged EXEC User EXEC

TABLE 3-4 Entry Definitions for `show spanning-tree mst port summary`

Entry	Definition
MST Instance ID	The MST instance associated with this port.
Interface	Valid slot and port number separated by forward slashes.
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.
Link Status	The operational status of the link. Possible values are “Up” or “Down”.
Link Trap	The link trap configuration for the specified interface.

`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**
Modes	Privileged EXEC User EXEC

TABLE 3-5 Entry Definitions for `show spanning-tree mst summary`

Entry	Definition
MST Instance ID List	List of multiple spanning trees IDs currently configured.

For each MSTID, the following will be displayed.

TABLE 3-6 Entry Definitions for `show spanning-tree mst summary` for Each MTSID

Display	Definition
Associated FIDs	List of forwarding database identifiers associated with this instance.
Associated VLANs	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**
Modes	Privileged EXEC User EXEC

TABLE 3-7 Entry Definitions for `show spanning-tree summary`

Entry	Definition
Spanning Tree Adminmode	Enabled or disabled.
Spanning Tree Version	Version of 802.1 currently supported (IEEE 802.1s, IEEE 802.1w, or IEEE 802.1d) based upon the Force Protocol Version parameter.
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	Identifier used to identify the configuration currently being used.
MST Instances	List of all multiple spanning tree instances configured on the switch

`show spanning-tree vlan`

This command displays the association between a VLAN and a multiple spanning tree instance. The *`<vlanid>`* corresponds to an existing VLAN ID.

Format	**show spanning-tree vlan** *<vlanid>*
Modes	Privileged EXEC User EXEC

TABLE 3-8 Entry Definitions for `show spanning-tree vlan`

Entry	Definition
VLAN Identifier	VLANs associated with the selected MST instance.
Associated Instance	Identifier for the associated multiple spanning tree instance or "CST" if associated with the common and internal spanning tree

Virtual LAN (VLAN) Commands

This section describes the commands you use to configure VLAN settings.

`vlan database`

This command gives you access to the VLAN Config mode, which allows you to configure VLAN characteristics.

Format	**`vlan database`**
Mode	Privileged EXEC

network mgmt_vlan

This command configures the Management VLAN ID.

Default	1
Format	**`network mgmt_vlan`** *<1-4069>*
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 2-3965.

Format	**vlan** *<2-3965>*
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). VLAN range is 2-3965.

Format	**no vlan** *<2-3965>*
Mode	VLAN Config

vlan acceptframe

This command sets the frame acceptance mode per interface. For VLAN Only mode, untagged frames or priority frames received on this interface are discarded. For Admit All mode, untagged frames or priority frames received on this interface are accepted and assigned the value of the interface VLAN ID for this port. With either option, VLAN tagged frames are forwarded in accordance with the IEEE 802.1Q VLAN Specification.

Default	all
Format	**vlan acceptframe** *{vlanonly | all}*
Mode	Interface Config

no vlan acceptframe

This command sets the frame acceptance mode per interface 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	**vlan acceptframe** *{vlanonly | all}*
Mode	Interface Config

vlan ingressfilter

This command enables 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.

Default	disabled
Format	**vlan ingressfilter**
Mode	Interface Config

no vlan ingressfilter

This command disables ingress filtering. If ingress filtering is disabled, frames received with VLAN IDs that do not match the VLAN membership of the receiving interface are admitted and forwarded to ports that are members of that VLAN.

Format	**no vlan ingressfilter**
Mode	Interface Config

vlan makestatic

This command changes a dynamically created VLAN (one that is 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 2-3965.

Format	**vlan makestatic** *<2-3965>*
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 1-4094.

Default	VLAN ID 1 - default other VLANS - blank string
Format	**vlan name** *<2-3965> <name>*
Mode	VLAN Config

`no vlan name`

This command sets the name of a VLAN to a blank string. The VLAN ID is a vailid VLAN identification number. ID range is 1-4094.

Format	**no vlan name** *<2-3965>*
Mode	VLAN Config

`vlan participation`

This command configures the degree of participation for a specific interface 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} <1-4094>*
Mode	Interface Config

Participation options are as follows.

TABLE 3-9 Entry Definitions for `vlan participation`

Entry	Definition
include	The interface is always a member of this VLAN. This is equivalent to registration fixed.
exclude	The interface is never a member of this VLAN. This is equivalent to registration forbidden.
auto	The interface is dynamically registered in this VLAN by GVRP. The interface 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} <1-4094>*
Mode	Global Config

Participation options are as follows.

TABLE 3-10 Entry Definitions for `vlan participation all`

Entry	Definition
include	The interface is always a member of this VLAN. This is equivalent to registration fixed.
exclude	The interface is never a member of this VLAN. This is equivalent to registration forbidden.
auto	The interface is dynamically registered in this VLAN by GVRP. 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. For VLAN Only mode, untagged frames or priority frames received on this interface are discarded. For Admit All mode, untagged frames or priority frames received on this interface are accepted and assigned the value of the interface VLAN ID for this port. With either option, VLAN tagged frames are forwarded in accordance with the IEEE 802.1Q VLAN Specification.

Default	all
Format	**vlan port acceptframe all** *{vlanonly | all}*
Mode	Global Config

`no vlan port acceptframe all`

This command sets the frame acceptance mode for all interfaces to Admit All. For Admit All mode, untagged frames or priority frames received on this interface are accepted and assigned the value of the interface VLAN ID for this port. With either option, VLAN tagged frames are forwarded in accordance with the IEEE 802.1Q VLAN Specification.

Format	**no vlan port acceptframe all**
Mode	Global Config

vlan port ingressfilter all

This command enables ingress filtering for all ports. If ingress filtering is disabled, frames received with VLAN IDs that do not match the VLAN membership of the receiving interface are admitted and forwarded to ports that are members of that VLAN.

Default	disabled
Format	**vlan port ingressfilter all**
Mode	Global Config

no vlan port ingressfilter all

This command disables ingress filtering for all ports. If ingress filtering is disabled, frames received with VLAN IDs that do not match the VLAN membership of the receiving interface are admitted and forwarded to ports that are members of that VLAN.

Format	**no vlan port ingressfilter all**
Mode	Global Config

vlan port pvid all

This command changes the VLAN ID for all interface.

Default	1
Format	**vlan port pvid all** *<1-4094>*
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** *<1-4094>*
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 group to the system. The <groupName> is a character string of 1 to 16 characters. When it is created, the protocol group will be assigned a unique number that will be used to identify the group in subsequent commands.

Format	**vlan protocol group** *<groupname>*
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 will fail and the protocol will not be added to the group. The possible values for protocol are ip, arp, and ipx.

Note – FASTPATH supports IPv4 protocol-based VLANs.

Default	none
Format	**vlan protocol group add protocol** *<groupid> <protocol>*
Mode	Global Config

no vlan protocol group add protocol

This command removes the <protocol> from this protocol-based VLAN group that is identified by this <groupid>. The possible values for protocol are ip, arp, and ipx.

Format	**no vlan protocol group add protocol** *<groupid> <protocol>*
Mode	Global Config

vlan protocol group remove

This command removes the protocol-based VLAN group that is identified by this <groupid>.

Format	**vlan protocol group remove** *<groupid>*
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.

The referenced VLAN should be created prior to the creation of the protocol-based VLAN except when GVRP is expected to create the VLAN.

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 the physical <slot/port> interface to the protocol-based VLAN identified by <groupid>. A group may have more than one interface associated with it. Each interface and protocol combination can only be associated 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.

The referenced VLAN should be created prior to the creation of the protocol-based VLAN except when GVRP is expected to create the VLAN.

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>. If <all> is selected, all ports will be removed from this protocol group.

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>. A group may have more than one interface associated with it. Each interface and protocol combination can only be associated 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.

The referenced VLAN should be created prior to the creation of the protocol-based VLAN except when GVRP is expected to create the VLAN.

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

vlan pvid

This command changes the VLAN ID per interface.

Default	1
Format	**vlan pvid** *<1-4094>*
Mode	Interface Config

no vlan pvid

This command sets the VLAN ID per interface to 1.

Format	**no vlan pvid**
Mode	Interface Config

vlan tagging

This command configures the tagging behavior for a specific interface 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** *<1-4094>*
Mode	Interface Config

no vlan tagging

This command configures the tagging behavior for a specific interface 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** *<1-4094>*
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

`show vlan`

This command displays detailed information, including interface information, for a specific VLAN. The ID is a valid VLAN identification number.

Format	**`show vlan`** *`<vlanid>`*
Modes	Privileged EXEC User EXEC

TABLE 3-11 Entry Definitions for `show vlan`

Entry	Definition
VLAN ID	There is a VLAN Identifier (VID) associated with each VLAN. The range of the VLAN ID is 1 to 4094.
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 (one that is created by GVRP registration).
Interface	Valid slot and port number separated by forward slashes. It is possible to set the parameters for all ports by using the selectors on the top line.

TABLE 3-11 Entry Definitions for `show vlan` *(Continued)*

Entry	Definition
Current	Determines the degree of participation of this port in this VLAN. The permissible values are as follows: • **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** - Specifies 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	Determines the configured degree of participation of this port in this VLAN. The permissible values are as follows: • **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 - Specifies 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	Select the tagging behavior for this port in this VLAN. • **Tagged** - specifies to transmit traffic for this VLAN as tagged frames. • **Untagged** - specifies to transmit traffic for this VLAN as untagged frames.

show vlan brief

This command displays a list of all configured VLANs.

Format	**`show vlan brief`**
Modes	Privileged EXEC User EXEC

TABLE 3-12 Entry Definitions for `show vlan` brief

Entry	Definition
VLAN ID	There is a VLAN Identifier (vlanid) associated with each VLAN. The range of the VLAN ID is 1 to 4094.
VLAN Name	A string associated with this VLAN as a convenience. It can be up to 32 alphanumeric characters long, including blanks. The default is blank. VLAN ID 1 always has a name of “Default.” This field is optional.
VLAN Type	Type of VLAN, which can be Default (VLAN ID = 1) or static (one that is configured and permanently defined), or a Dynamic (one that is created by GVRP registration).

show vlan port

This command displays VLAN port information.

Format	**`show vlan port`** *`{<slot/port>	all}`*
Modes	Privileged EXEC User EXEC

TABLE 3-13 Entry Definitions for `show vlan` port

Entry	Definition
Interface	Valid slot and port number separated by forward slashes. It is possible to set the parameters for all ports by using the selectors on the top line.
Port VLAN ID	The VLAN ID that this port will assign to untagged frames or priority tagged frames received on this port. The value must be for an existing VLAN. The factory default is 1.
Acceptable Frame Types	Specifies 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.

TABLE 3-13 Entry Definitions for `show vlan` port *(Continued)*

Entry	Definition
Ingress Filtering	May be enabled or disabled. When enabled, the frame is discarded if this port is not a member of the VLAN with which this frame is associated. In a tagged frame, the VLAN is identified by the VLAN ID in the tag. In an untagged frame, the VLAN is the Port VLAN ID specified for the port that received this frame. When disabled, all frames are forwarded in accordance with the 802.1Q VLAN bridge specification. The factory default is disabled.
GVRP	May be enabled or disabled.
Default Priority	The 802.1p priority assigned to tagged packets arriving on the port.

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

TABLE 3-14 Entry Definitions for `show vlan` association subnet

Entry	Definition
IP Address	The IP address assigned to each interface.
Net Mask	The subnet mask
VLAN ID	There is a VLAN Identifier (VID) associated with each VLAN.

show vlan association mac

This command displays the VLAN associated with a specific configured MAC address. If no MAC address is specified, the VLAN associations of all the configured MAC addresses are displayed.

Format	**`show vlan association mac`** *`[<macaddr>]`*
Mode	Privileged EXEC

TABLE 3-15 Entry Definitions for `show vlan` association mac

Entry	Definition
Mac Address	A MAC address for which the switch has forwarding and or filtering information. The format is 6 or 8 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB. In an IVL system the MAC address will be displayed as 8 bytes.
VLAN ID	There is a VLAN Identifier (VID) associated with each VLAN.

Double VLAN Commands

This section describes the commands you use to configure double VLAN (DVLAN). Double VLAN tagging is a way to pass VLAN traffic from one customer domain to another through a Metro Core in a simple and cost effective manner. The additional tag on the traffic helps differentiate between customers in the MAN while preserving the VLAN identification of the individual customers when they enter their own 802.1Q domain.

`dvlan-tunnel etherType`

This command configures the ether-type for the specified interface. The ether-type may have the values of 802.1Q, vMAN, or custom. If the ether-type has a value of custom, the optional value of the custom ether type must be set to a value from 0 to 65535.

Default	vman
Format	**dvlan-tunnel ethertype** *{802.1Q | vman | custom} [0-65535]*
Mode	Global Config

`no dvlan-tunnel etherType`

This command configures the ether-type for the specified interface to its default value.

Format	**no dvlan-tunnel ethertype**
Mode	Global Config

mode dot1q-tunnel

This command is used to enable Double VLAN Tunneling on the specified interface. By default, Double VLAN Tunneling is disabled.

Default	disabled
Format	**mode dot1q-tunnel**
Mode	Interface Config

no mode dot1q-tunnel

This command is used to disable Double VLAN Tunneling on the specified interface. By default, Double VLAN Tunneling is disabled.

Format	**no mode dot1q-tunnel**
Mode	Interface Config

mode dvlan-tunnel

Use this command to enable Double VLAN Tunneling on the specified interface. By default, Double VLAN Tunneling is disabled.

Default	disabled
Format	**mode dvlan-tunnel**
Mode	Interface Config

Note – When you use the `mode dvlan-tunnel` command on an interface, it becomes a service provider port. Ports that do not have double VLAN tunneling enabled are customer ports.

no mode dvlan-tunnel

This command is used to disable Double VLAN Tunneling on the specified interface. By default, Double VLAN Tunneling is disabled.

Format	**no mode dvlan-tunnel**
Mode	Interface Config

show dot1q-tunnel

Use this command without the optional parameters to display all interfaces enabled for Double VLAN Tunneling. Use the optional parameters to display detailed information about Double VLAN Tunneling for the specified interface or all interfaces.

Format	**`show dot1q-tunnel`** *`[interface {<slot/port>	all}]`*
Modes	Privileged EXEC User EXEC

TABLE 3-16 Entry Definitions for `show dot1q-tunnel`

Entry	**Definition**
Interface	Valid slot and port number separated by forward slashes.
Mode	This field specifies the administrative mode through which Double VLAN Tunneling can be enabled or disabled. The default value for this field is disabled.
EtherType	This field represents a 2-byte hex EtherType to be used as the first 16 bits of the DVLAN tunnel. There are three different EtherType tags. The first is 802.1Q, which represents the commonly used value of 0x8100. The second is vMAN, which represents the commonly used value of 0x88A8. If EtherType is not one of these two values, then it is a custom tunnel value, representing any value in the range of 0 to 65535.

show dvlan-tunnel

Use this command without the optional parameters to display all interfaces enabled for Double VLAN Tunneling. Use the optional parameters to display detailed information about Double VLAN Tunneling for the specified interface or all interfaces.

Format	**`show dvlan-tunnel`** *`[interface {<slot/port> | all}]`*
Modes	Privileged EXEC User EXEC

TABLE 3-17 Entry Definitions for `show dvlan-tunnel`

Entry	Definition
Interface	Valid slot and port number separated by forward slashes.
Mode	This field specifies the administrative mode through which Double VLAN Tunneling can be enabled or disabled. The default value for this field is disabled.
EtherType	This field represents a 2-byte hex EtherType to be used as the first 16 bits of the DVLAN tunnel. There are three different EtherType tags. The first is 802.1Q, which represents the commonly used value of 0x8100. The second is vMAN, which represents the commonly used value of 0x88A8. If EtherType is not one of these two values, then it is a custom tunnel value, representing any value in the range of 0 to 65535.

Provisioning (IEEE 802.1p) Commands

This section describes the commands you use to configure provisioning, 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

Protected Ports Commands

This section describes commands you use to configure and view protected ports on a switch. Protected ports do not forward traffic to each other, even if they are on the same VLAN. However, protected ports can forward traffic to all unprotected ports in their group. Unprotected ports can forward traffic to both protected and unprotected ports. Ports are unprotected by default.

If an interface is configured as a protected port, and you add that interface to a Port Channel or Link Aggregation Group (LAG), the protected port status becomes operationally disabled on the interface, and the interface follows the configuration of the LAG port. However, the protected port configuration for the interface remains unchanged. Once the interface is no longer a member of a LAG, the current configuration for that interface automatically becomes effective.

switchport protected (Global Config)

Use this command to create a protected port group. The *`<groupid>`* parameter identifies the set of protected ports. Use the *`name <name>`* pair to assign a name to the protected port group. The name can be up to 32 alphanumeric characters long, including blanks. The default is blank.

Note – Port protection occurs within a single switch. Protected port configuration does not affect traffic between ports on two different switches. No traffic forwarding is possible between two protected ports.

Default	unprotected
Format	**`switchport protected`** *`<groupid> [name <name>]`*
Mode	Global Config

no switchport protected (Global Config)

Use this command to remove a protected port group. The *`groupid`* parameter identifies the set of protected ports. Use the **`name`** keyword to remove the name 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>*
Modes	Privileged EXEC User EXEC

TABLE 3-18 Entry Definitions for `show switchport protected`

Entry	Definition
Group ID	The number that identifies the protected port group.
Name	An optional name of the protected port group. The name can be up to 32 alphanumeric characters long, including blanks. The default is blank.
List of Physical Ports	List of ports, which are configured as protected for the group identified with *<groupid>*. If no port is configured as protected for this group, this field is blank.

show interfaces switchport

This command displays the status of the interface (protected/unprotected) under the groupid.

Format	**show interfaces switchport** *<slot/port> <groupid>*
Mode	User EXEC Privileged EXEC

TABLE 3-19 Entry Definitions for

Entry	**Definition**
Name	A string associated with this group as a convenience. It can be up to 32 alphanumeric characters long, including blanks. The default is blank. This field is optional.
Protected	Indicates whether the interface is protected or not. It shows TRUE or FALSE. If the group is a multiple groups then it shows TRUE in Group *<groupid>*

GARP Commands

This section describes the commands you use to configure Generic Attribute Registration Protocol (GARP) and view GARP status. The commands in this section affect both GARP VLAN Registration Protocol (GVRP) and Garp Multicast Registration Protocol (GMRP). GARP is a protocol that allows client stations to register with the switch for membership in VLANS (by using GVMP) or multicast groups (by using GVMP).

`set garp timer join`

This command sets the GVRP join time for one port (Interface Config mode) or all (Global Config mode) and per GARP. Join time is the interval between the transmission of GARP Protocol Data Units (PDUs) registering (or re-registering) membership for a VLAN or multicast group. This command has an effect only when GVRP is enabled. The time is from 10 to 100 (centiseconds). The value 20 centiseconds is 0.2 seconds.

Default	20
Format	*`set garp timer join <10-100>`*
Modes	Interface Config Global Config

no set garp timer join

This command sets the GVRP join time (for one or all ports and per GARP) to the default and only has an effect when GVRP is enabled.

Format	*`no set garp timer join`*
Modes	Interface Config Global Config

set garp timer leave

This command sets the GVRP leave time for one port (Interface Config mode) or all ports (Global Config mode) 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.

Default	60
Format	**`set garp timer leave`** *`<20-600>`*
Modes	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`**
Modes	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 a single port (Interface Config mode), and it only has an effect only when GVRP is enabled.

Default	1000
Format	**`set garp timer leaveall`** *<200-6000>*
Modes	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`**
Modes	Interface Config Global Config

show garp

This command displays GARP information.

Format	**`show garp`**
Modes	Privileged EXEC User EXEC

TABLE 3-20 Entry Definitions for `show garp`

Entry	Definition
GMRP Admin Mode	This displays the administrative mode of GARP Multicast Registration Protocol (GMRP) for the system.
GVRP Admin Mode	This displays the administrative mode of GARP VLAN Registration Protocol (GVRP) for the system

GVRP Commands

This section describes the commands you use to configure and view GARP VLAN Registration Protocol (GVRP) information. GVRP-enabled switches exchange VLAN configuration information, which allows GVRP to provide dynamic VLAN creation on trunk ports and automatic VLAN pruning.

Note – If GVRP is disabled, the system does not forward GVRP messages.

`set gvrp adminmode`

This command enables GVRP on the system.

Default	disabled
Format	**`set gvrp adminmode`**
Mode	Privileged EXEC

`no set gvrp adminmode`

This command disables GVRP.

Format	**`no set gvrp adminmode`**
Mode	Privileged EXEC

set gvrp interfacemode

This command enables GVRP on a single port (Interface Config mode) or all ports (Global Config mode).

Default	disabled
Format	**`set gvrp interfacemode`**
Modes	Interface Config 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`**
Modes	Interface Config Global Config

show gvrp configuration

This command displays Generic Attributes Registration Protocol (GARP) information for one or all interfaces.

Format	**`show gvrp configuration`** *`{<slot/port> | all}`*
Modes	Privileged EXEC User EXEC

TABLE 3-21 Entry Definitions for `show gvrp configuration`

Entry	Definition
Interface	Valid slot and port number separated by forward slashes.
Join Timer	Specifies the interval between the transmission of GARP PDUs registering (or re-registering) membership for an attribute. Current attributes are a VLAN or multicast group. There is an instance of this timer on a per-Port, per-GARP participant basis. Permissible 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	Specifies 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	Indicates the GMRP administrative mode for the port, which is enabled or disabled (default). If this parameter is disabled, Join Time, Leave Time and Leave All Time have no effect.

GMRP Commands

This section describes the commands you use to configure and view GARP Multicast Registration Protocol (GMRP) information. Like IGMP snooping, GMRP helps control the flooding of multicast packets.GMRP-enabled switches dynamically register and de-register group membership information with the MAC networking devices attached to the same segment. GMRP also allows group membership information to propagate across all networking devices in the bridged LAN that support Extended Filtering Services.

Note – If GMRP is disabled, the system does not forward GMRP messages.

`set gmrp adminmode`

This command enables GARP Multicast Registration Protocol (GMRP) on the system.

Default	disabled
Format	**`set gmrp adminmode`**
Mode	Privileged EXEC

`no set gmrp adminmode`

This command disables GARP Multicast Registration Protocol (GMRP) on the system.

Format	**`no set gmrp adminmode`**
Mode	Privileged EXEC

`set gmrp interfacemode`

This command enables GARP Multicast Registration Protocol on a single interface (Interface Config mode) 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`**
Modes	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`**
Modes	Interface Config Global Config

show gmrp configuration

This command displays Generic Attributes Registration Protocol (GARP) information for one or all interfaces.

Format	**`show gmrp configuration`** *`{<slot/port> | all}`*
Modes	Privileged EXEC User EXEC

TABLE 3-22 Entry Definitions `show gmrp configuration`

Entry	**Definition**
Interface	This displays the slot/port of the interface that this row in the table describes.
Join Timer	Specifies the interval between the transmission of GARP PDUs registering (or re-registering) membership for an attribute. Current attributes are a VLAN or multicast group. There is an instance of this timer on a per-port, per-GARP participant basis. Permissible 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).

TABLE 3-22 Entry Definitions `show gmrp configuration` *(Continued)*

Entry	Definition
Leave Timer	Specifies 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	Indicates 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

TABLE 3-23 Entry Definitions for `show mac-address-table gmrp`

Entry	Definition
Mac Address	A unicast MAC address for which the switch has forwarding and or filtering information. The format is 6 or 8 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB. In an IVL system the MAC address is displayed as 8 bytes.

TABLE 3-23 Entry Definitions for `show mac-address-table gmrp`

Entry	Definition
Type	Displays the type of the entry. Static entries are those that are configured by the end user. Dynamic entries are added to the table as a result of a learning process or protocol.
Description	The text description of this multicast table entry.
Interfaces	The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).

Port-Based Network Access Control Commands

This section describes the commands you use to configure port-based network access control (802.1x). Port-based network access control allows you to permit access to network services only to and devices that are authorized and authenticated.

`authentication login`

This command creates an authentication login list. The *`<listname>`* is any character string and is not case sensitive. Up to 10 authentication login lists can be configured on the switch. When a list is created, the authentication method "local" is set as the first method.

When the optional parameters "Option1", "Option2" and/or "Option3" are used, an ordered list of methods are set in the authentication login list. If the authentication login list does not exist, a new authentication login list is first created and then the authentication methods are set in the authentication login list. The maximum number of authentication login methods is three. The possible method values are `local, radius` and `reject`.

The value of `local` indicates that the user's locally stored ID and password are used for authentication. The value of `radius` indicates that the user's ID and password will be authenticated using the RADIUS server. The value of `reject` indicates the user is never authenticated.

To authenticate a user, the first authentication method in the user's login (authentication login list) is attempted. FASTPATH software does not utilize multiple entries in the user's login. If the first entry returns a timeout, the user authentication attempt fails.

Note – The default login list included with the default configuration can not be changed.

Format	**`authentication login`** *`<listname> [<method1> [<method2> [<method3>]]]`*
Mode	Global Config

no authentication login

This command deletes the specified authentication login list. The attempt to delete fails if any of the following conditions are true:

- The login list name is invalid or does not match an existing authentication login list
- The specified authentication login list is assigned to any user or to the non configured user for any component
- The login list is the default login list included with the default configuration and was not created using 'authentication login'. The default login list cannot be deleted.

Format	**`no authentication login`** *`<listname>`*
Mode	Global Config

clear dot1x statistics

This command resets the 802.1x statistics for the specified port or for all ports.

Format	**`clear dot1x statistics`** *`{<slot/port> | all}`*
Mode	Privileged EXEC

clear radius statistics

This command is used to clear all RADIUS statistics.

Format	**`clear radius statistics`**
Mode	Privileged EXEC

dot1x defaultlogin

This command assigns the authentication login list to use for non-configured users for 802.1x port security. This setting is over-ridden by the authentication login list assigned to a specific user if the user is configured locally. If this value is not configured, users will be authenticated using local authentication only.

Format	**`dot1x defaultlogin`** *`<listname>`*
Mode	Global Config

dot1x initialize

This command begins the initialization sequence on the specified port. This command is only valid if the control mode for the specified port is 'auto'. If the control mode is not 'auto' an error will be returned.

Format	**`dot1x initialize`** *`<slot/port>`*
Mode	Privileged EXEC

dot1x login

This command assigns the specified authentication login list to the specified user for 802.1x port security. The *`<user>`* parameter must be a configured user and the *`<listname>`* parameter must be a configured authentication login list.

Format	**`dot1x login`** *`<user> <listname>`*
Mode	Global Config

dot1x max-req

This command sets the maximum number of times the authenticator state machine on this port will transmit an EAPOL EAP Request/Identity frame before timing out the supplicant. The `<count>` value must be in the range 1 - 10.

Default	2
Format	**`dot1x max-req`** *`<count>`*
Mode	Interface Config

no dot1x max-req

This command sets the maximum number of times the authenticator state machine on this port will transmit an EAPOL EAP Request/Identity frame before timing out the supplicant.

Format	**`no dot1x max-req`**
Mode	Interface Config

dot1x port-control

This command sets the authentication mode to use on the specified port. 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.

Default	auto
Format	**`dot1x port-control`** *`{force-unauthorized	force-authorized	auto}`*
Mode	Interface Config

no dot1x port-control

This command sets the authentication 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.

Default	auto
Format	**`dot1x port-control all`** *`{force-unauthorized | force-authorized | auto}`*
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 re-authenticate

This command begins the re-authentication sequence on the specified port. This command is only valid if the control mode for the specified port is 'auto'. If the control mode is not 'auto' an error will be returned.

Format	**`dot1x re-authenticate`** *`<slot/port>`*
Mode	Privileged EXEC

dot1x re-authentication

This command enables re-authentication of the supplicant for the specified port.

Default	disabled
Format	**`dot1x re-authentication`**
Mode	Interface Config

no dot1x re-authentication

This command disables re-authentication of the supplicant for the specified port.

Format	**`no dot1x re-authentication`**
Mode	Interface Config

dot1x system-auth-control

Use this command to enable the dot1x authentication support on the switch. While disabled, the dot1x configuration is retained and can be changed, but is not activated.

Default	disabled
Format	**`dot1x system-auth-control`**
Mode	Global Config

no dot1x system-auth-control

This command is used to disable the dot1x authentication support on the switch.

Format	**`no dot1x system-auth-control`**
Mode	Global Config

dot1x timeout

This command sets the value, in seconds, of the timer used by the authenticator state machine on this port. Depending on the token used and the value (in seconds) passed, various timeout configurable parameters are set. The following tokens are supported.

reauth-period: Sets the value, in seconds, of the timer used by the authenticator state machine on this port to determine when re-authentication of the supplicant takes place. The reauth-period must be a value in the range 1 - 65535.

quiet-period: Sets the value, in seconds, of the timer used by the authenticator state machine on this port to define periods of time in which it will not attempt to acquire a supplicant. The quiet-period must be a value in the range 0 - 65535.

tx-period: Sets the value, in seconds, of the timer used by the authenticator state machine on this port to determine when to send an EAPOL EAP Request/Identity frame to the supplicant. The quiet-period must be a value in the range 1 - 65535.

supp-timeout: Sets the value, in seconds, of the timer used by the authenticator state machine on this port to timeout the supplicant. The supp-timeout must be a value in the range 1 - 65535.

server-timeout: Sets the value, in seconds, of the timer used by the authenticator state machine on this port to timeout the authentication server. The supp-timeout must be a value in the range 1 - 65535.

Default	reauth-period: 3600 seconds quiet-period: 60 seconds tx-period: 30 seconds supp-timeout: 30 seconds server-timeout: 30 seconds
Format	**`dot1x timeout`** *`{{reauth-period <seconds>} | {quiet-period <seconds>} | {tx-period <seconds>} | {supp-timeout <seconds>} | {server-timeout <seconds>}}`*
Mode	Interface Config

no dot1x timeout

This command sets the value, in seconds, of the timer used by the authenticator state machine on this port to the default values. Depending on the token used, the corresponding default values are set.

Format	**`no dot1x timeout`** *`{reauth-period	quiet-period	tx-period	supp-timeout	server-timeout}`*
Mode	Interface Config

dot1x user

This command adds the specified user to the list of users with access to the specified port or all ports. The *`<user>`* parameter must be a configured user.

Format	**`dot1x user`** *`<user> {<slot/port>	all}`*
Mode	Global Config

no dot1x user

This command removes the user from the list of users with access to the specified port or all ports.

Format	**`no dot1x user`** *`<user> {<slot/port>	all}`*
Mode	Global Config

users defaultlogin

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

Format	**`users defaultlogin`** *`<listname>`*
Mode	Global Config

`users login`

This command assigns the specified authentication login list to the specified user for system login. The *`<user>`* must be a configured *`<user>`* and the *`<listname>`* must be a configured login list.

If the user is assigned a login list that requires remote authentication, all access to the interface from all CLI, web, and telnet sessions will be blocked until the authentication is complete.

Note that the login list associated with the 'admin' user can not be changed to prevent accidental lockout from the switch.

Format	**`users login`** *`<user> <listname>`*
Mode	Global Config

`show authentication`

This command displays the ordered authentication methods for all authentication login lists.

Format	**`show authentication`**
Mode	Privileged EXEC

TABLE 3-24 Entry Definitions for `show authentication`

Entry	Definition
Authentication Login List	This displays the authentication login listname.
Method 1	This displays the first method in the specified authentication login list, if any.
Method 2	This displays the second method in the specified authentication login list, if any.
Method 3	This displays the third method in the specified authentication login list, if any.

show authentication users

This command displays information about the users assigned to the specified authentication login list. If the login is assigned to non-configured users, the user “default” will appear in the user column.

Format	**`show authentication users`** *`<listname>`*
Mode	Privileged EXEC
User	This field displays the user assigned to the specified authentication login list.
Component	This field displays the component (User or 802.1x) for which the authentication login list is assigned.

show dot1x

This command is used to show a summary of the global dot1x configuration, summary information of the dot1x configuration for a specified port or all ports, the detailed dot1x configuration for a specified port and the dot1x statistics for a specified port - depending on the tokens used.

Format	**`show dot1x`** *`[{summary {<slot/port>	all}	detail <slot/port>	statistics <slot/port>]`*
Mode	Privileged EXEC

If you do not use any of the optional parameters, the global dot1x configuration summary is displayed.

Administrative mode	Indicates whether authentication control on the switch is enabled or disabled.

If you use the optional parameter *summary {<slot/port> | all}*, the dot1x configuration for the specified port or all ports are displayed.

TABLE 0-3 Entry Definitions for `show dot1x` *summary {<slot/port> | all}*

Entry	**Definition**
Port	The interface whose configuration is displayed.
Control Mode	The configured control mode for this port. Possible values are force-unauthorized | force-authorized | auto.
Operating Control Mode	The control mode under which this port is operating. Possible values are authorized | unauthorized.
Reauthentication Enabled	Indicates whether re-authentication is enabled on this port.
Key Transmission Enabled	Indicates if the key is transmitted to the supplicant for the specified port.

If the optional parameter `detail` *<slot/port>* is used, the detailed dot1x configuration for the specified port are displayed.

TABLE 3-25 Entry Definitions for `show dot1x` *detail {<slot/port> | all}*

Entry	**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.
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.
Quiet Period	The timer used by the authenticator state machine on this port to define periods of time in which it will not attempt to acquire a supplicant. The value is expressed in seconds and will be in the range 0 and 65535.
Transmit Period	The timer used by the authenticator state machine on the specified port to determine when to send an EAPOL EAP Request/Identity frame to the supplicant. The value is expressed in seconds and will be in the range of 1 and 65535.

TABLE 3-25 Entry Definitions for `show dot1x` *`detail {<slot/port> | all}`*

Entry	Definition
Supplicant Timeout	The timer used by the authenticator state machine on this port to timeout the supplicant. The value is expressed in seconds and will be in the range of 1 and 65535.
Server Timeout	The timer used by the authenticator on this port to timeout the authentication server. The value is expressed in seconds and will be in the range of 1 and 65535.
Maximum Requests	The maximum number of times the authenticator state machine on this port will retransmit an EAPOL EAP Request/Identity before timing out the supplicant. The value will be in the range of 1 and 10.
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	Indicates if reauthentication is enabled on this port. Possible values are 'True" or "False".
Key Transmission Enabled	Indicates if the key is transmitted to the supplicant for the specified port. Possible values are True or False.
Control Direction	Indicates the control direction for the specified port or ports. Possible values are both or in.

If you use the optional parameter *`statistics <slot/port>`*, the following dot1x statistics for the specified port appear.

TABLE 3-26 Entry Definitions for `show dot1x` *`statistics {<slot/port> | all}`*

Entry	Definition
Port	The interface whose statistics are displayed.
EAPOL Frames Received	The number of valid EAPOL frames of any type that have been received by this authenticator.
EAPOL Frames Transmitted	The number of EAPOL frames of any type that have been transmitted by this authenticator.
EAPOL Start Frames Received	The number of EAPOL start frames that have been received by this authenticator.
EAPOL Logoff Frames Received	The number of EAPOL logoff frames that have been received by this authenticator.
Last EAPOL Frame Version	The protocol version number carried in the most recently received EAPOL frame.
Last EAPOL Frame Source	The source MAC address carried in the most recently received EAPOL frame.

TABLE 3-26 Entry Definitions for `show dot1x` *`statistics {<slot/port> | all}`*

Entry	Definition
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 users

This command displays 802.1x port security user information for locally configured users.

Format	**`show dot1x users`** *`<slot/port>`*
Mode	Privileged EXEC
User	Users configured locally to have access to the specified port.

`show users authentication`

This command displays all user and all authentication login information. It also displays the authentication login list assigned to the default user.

Format	**`show users authentication`**
Mode	Privileged EXEC
User	Lists every user that has an authentication login list assigned.
System Login	Displays the authentication login list assigned to the user for system login.
802.1x Port Security	This field displays the authentication login list assigned to the user for 802.1x port security.

Storm-Control Commands

This section describes commands you use to configure storm control and view storm-control configuration information. 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. The Storm Control feature can help maintain network performance.

`storm-control broadcast`

Use this command to enable broadcast storm recovery mode for a specific interface. 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	Interface Config

no storm-control broadcast

Use this command to disable broadcast storm recovery mode for a specific interface.

Format	**`no storm-control broadcast`**
Mode	Interface Config

storm-control broadcast level

Use this command to configure the broadcast storm recovery threshold for an interface. When you use this command, broadcast storm recovery mode is enabled on the interface and broadcast storm recovery is active. 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	Interface Config

no storm-control broadcast level

This command sets the broadcast storm recovery threshold to the default value for an interface and disables broadcast storm recovery.

Format	**`no storm-control broadcast level`**
Mode	Interface Config

storm-control broadcast all

This command enables broadcast storm recovery mode for all interfaces. 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 all`**
Mode	Global Config

no storm-control broadcast all

This command disables broadcast storm recovery mode for all interfaces.

Format	**`no storm-control broadcast all`**
Mode	Global Config

storm-control broadcast all level

This command configures the broadcast storm recovery threshold for all interfaces. 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.This command also enables broadcast storm recovery mode for all interfaces.

Default	5
Format	**`storm-control broadcast all level`** <0-100>
Mode	Global Config

no storm-control broadcast all level

This command sets the broadcast storm recovery threshold to the default value for all interfaces and disables broadcast storm recovery.

Format	**`no storm-control broadcast all level`**
Mode	Global Config

storm-control multicast

This command enables multicast storm recovery mode for an interface. 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	Interface Config

no storm-control multicast

This command disables multicast storm recovery mode for an interface.

Format	**`no storm-control multicast`**
Mode	Interface Config

storm-control multicast level

This command configures the multicast storm recovery threshold for an interface 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	Interface Config

no storm-control multicast level

This command sets the multicast storm recovery threshold to the default value for an interface and disables multicast storm recovery.

Format	**`no storm-control multicast level`**
Mode	Interface Config

storm-control multicast all

This command enables multicast storm recovery mode for all interfaces. If the mode is enabled, multicast storm recovery is active, and if the rate of L2 multicast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of multicast traffic will be limited to the configured threshold.

Default	disabled
Format	**`storm-control multicast all`**
Mode	Global Config

no storm-control multicast all

This command disables multicast storm recovery mode for all interfaces.

Format	**`no storm-control multicast all`**
Mode	Global Config

storm-control multicast all level

This command configures the multicast storm recovery threshold for all interfaces 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 all level`** <0-100>
Mode	Global Config

no storm-control multicast all level

This command sets the multicast storm recovery threshold to the default value for all interfaces and disables multicast storm recovery.

Format	**`no storm-control multicast all level`**
Mode	Global Config

storm-control unicast

This command enables unicast storm recovery mode for an interface. 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	Interface Config

no storm-control unicast

This command disables unicast storm recovery mode for an interface.

Format	**`no storm-control unicast`**
Mode	Interface Config

storm-control unicast level

This command configures the unicast storm recovery threshold for an interface 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	Interface Config

no storm-control unicast level

This command sets the unicast storm recovery threshold to the default value for an interface and disables unicast storm recovery.

Format	**`no storm-control unicast level`**
Mode	Interface Config

storm-control unicast all

This command enables unicast storm recovery mode for all interfaces. If the mode is enabled, unicast storm recovery is active, and if the rate of unknown L2 unicast (destination lookup failure) traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of unknown unicast traffic will be limited to the configured threshold.

Default	disabled
Format	**`storm-control unicast all`**
Mode	Global Config

no storm-control unicast all

This command disables unicast storm recovery mode for all interfaces.

Format	**`no storm-control unicast all`**
Mode	Global Config

storm-control unicast all level

This command configures the unicast storm recovery threshold and enables unicast storm recovery for all interfaces. If the mode is enabled, unicast storm recovery is active, and if the rate of unknown L2 unicast (destination lookup failure) traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of unknown unicast traffic will be limited to the configured threshold.

Default	5
Format	**`storm-control unicast all level`** <0-100>
Mode	Global Config

no storm-control unicast all level

This command returns the unicast storm recovery threshold to the default value and disables unicast storm recovery for all interfaces.

Format	**`no storm-control unicast all level`**
Mode	Global Config

storm-control flowcontrol

This command enables 802.3x flow control for the switch and only applies to full-duplex mode ports.

Note – 802.3x flow control works by pausing a port when the port becomes oversubscribed and dropping all traffic for small bursts of time during the congestion condition. This can lead to high-priority and/or network control traffic loss.

Default	disabled
Format	**`storm-control flowcontrol`**
Mode	Global Config

`no storm-control flowcontrol`

This command disables 802.3x flow control for the switch.

Note – This command only applies to full-duplex mode ports.

Format	**`no storm-control flowcontrol`**
Mode	Global 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. Use the **`all`** keyword to display the per-port configuration parameters for all interfaces, or specify the *`slot/port`* to display information about a specific interface.

Format	**`show storm-control`** *`[all	<slot/port>]`*
Mode	Privileged EXEC

TABLE 3-27 Entry Definitions for `show storm-control`

Entry	Definition
Bcast Mode	Shows whether the broadcast storm control mode is enabled or disabled.
Bcast Level	Shows the broadcast storm control level.
Mcast Mode	Shows whether the multicast storm control mode is enabled or disabled.
Mcast Level	Shows 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	Shows the Unknown Unicast or DLF (Destination Lookup Failure) storm control level

Port-Channel/LAG (802.3ad) Commands

This section describes the commands you use to configure port-channels, which are also known as link aggregation groups (LAGs). Link aggregation allows you to combine multiple full-duplex Ethernet links into a single logical link. Network devices treat the aggregation as if it were a single link, which increases fault tolerance and provides load sharing. The LAG feature initially load shares traffic based upon the source and destination MAC address.Assign the port-channel (LAG) VLAN membership after you create a port-channel. If you do not assign VLAN membership, the port-channel might become a member of the management VLAN which can result in learning and switching issues.

A port-channel (LAG) interface can be either static or dynamic, but not both. All members of a port channel must participate in the same protocols.) A static port-channel interface does not require a partner system to be able to aggregate its member ports.

Note – If you configure the maximum number of 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 slot/port number for the port-channel. The *<name>* field is a character string which allows the dash "-" character as well as alphanumeric characters. Use the `show port channel` command to display the slot/port number for the logical interface.

Note – Before you include a port in a port-channel, set the port physical mode. For more information, see "speed" on page 34.

Format	**`port-channel`** *<name>*
Mode	Global Config

no port-channel

This command deletes a port-channel (LAG).

Format	**`no port-channel`** *`{<logical slot/port>	all}`*
Mode	Global Config

addport

This command adds one port to the port-channel (LAG). The first interface is a Logical slot and port number. of a configured port-channel.

Note – Before adding a port to a port-channel, set the physical mode of the port. For more information, see "speed" on page 34.

Format	**`addport`** *`<logical slot/port>`*
Mode	Interface Config

deleteport (Interface Config)

This command deletes the port from the port-channel (LAG). The interface is a Logical slot and port number. of a configured port-channel.

Format	**`deleteport`** *`<logical slot/port>`*
Mode	Interface Config

deleteport (Global Config)

This command deletes all configured ports from the port-channel (LAG). The interface is a Logical slot and port number. of a configured port-channel. To clear the port channels, see "clear port-channel" on page 445

Format	**`deleteport`** *`{<logical slot/port>	all}`*
Mode	Global Config

port-channel static

This command enables the static mode on a port-channel (LAG) interface. By default the static mode for a new port-channel is disabled, which means the port-channel is dynamic. However if the maximum number of allowable dynamic port-channels are already present in the system, the static mode for a new port-channel enabled, which means the port-channel is static.You can only use this command on port-channel interfaces.

Default	disabled
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.

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 all

This command enables Link Aggregation Control Protocol (LACP) on all ports.

Format	**`port lacpmode all`**
Mode	Global Config

no port lacpmode all

This command disables Link Aggregation Control Protocol (LACP) on all ports.

Format	**`no port lacpmode all`**
Mode	Global Config

port-channel adminmode

This command enables a port-channel (LAG). The option **`all`** sets every configured port-channel with the same administrative mode setting.

Format	**`port-channel adminmode`** *`[all]`*
Mode	Global Config

no port-channel adminmode

This command disables a port-channel (LAG). The option **`all`** sets every configured port-channel with the same administrative mode setting.

Format	**`no port-channel adminmode`** *`[all]`*
Mode	Global Config

port-channel linktrap

This command enables link trap notifications for the port-channel (LAG). The interface is a logical slot/port for a configured port-channel. The option **`all`** sets every configured port-channel with the same administrative mode setting.

Default	enabled
Format	**`port-channel linktrap`** *`{<logical slot/port> | all}`*
Mode	Global Config

no port-channel linktrap

This command disables link trap notifications for the port-channel (LAG). The interface is a logical slot and port for a configured port-channel. The option **`all`** sets every configured port-channel with the same administrative mode setting.

Format	**`no port-channel linktrap`** *`{<logical slot/port> | all}`*
Mode	Global Config

port-channel name

This command defines a name for the port-channel (LAG). The interface is a logical slot/port for a configured port-channel, and *<name>* is an alphanumeric string up to 15 characters.

Format	**`port-channel name`** *`{<logical slot/port> | all | <name>}`*
Mode	Global Config

show port-channel brief

This command displays a summary of individual port-channel (LAG) interfaces.

Format	**`show port-channel brief`**
Modes	Privileged EXEC User EXEC

For each port-channel the following information is displayed.

TABLE 3-28 Entry Definitions for `show port-channel brief`

Entry	**Definition**
Logical Interface	Shows the slot/port of the logical interface.
Port-channel Name	Shows the name of port-channel (LAG) interface.
Link-State	Shows whether the link is up or down.
Type	Shows whether the port-channel is statically or dynamically maintained.
Mbr Ports	Shows the members of this port-channel
Active Ports	Shows ports that are actively participating in the port-channel

show port-channel

This command displays an overview of all port-channels (LAGs) on the switch.

Format	**`show port-channel`** *`{<logical slot/port>	all}`*
Modes	Privileged EXEC User EXEC

TABLE 3-29 Entry Definitions for `show port-channel`

Entry	Definition
Logical Interface	Valid slot and port number separated by forward slashes.
Port-Channel Name	The name of this port-channel (LAG). You may enter any string of up to 15 alphanumeric characters.
Link State	Indicates whether the Link is up or down.
Admin Mode	May be enabled or disabled. The factory default is enabled.
Link Trap Mode	This object determines whether or not to send a trap when link status changes. The factory default is enabled.
STP Mode	The Spanning Tree Protocol Administrative Mode associated with the port or port-channel (LAG). The possible values are:as follows • **Disable** - Spanning tree is disabled for this port. • **Enable** - Spanning tree is enabled for this port.
Mbr Ports	A listing of the ports that are members of this port-channel (LAG), in slot/port notation. There can be a maximum of eight ports assigned to a given port-channel (LAG).
Port Speed	Speed of the port-channel port.
Type	This field displays 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.
Active Ports	This field lists ports that are actively participating in the port-channel (LAG).

Port Mirroring

Port mirroring, which is also known as port monitoring, selects network traffic that you can analyze with a network analyzer, such as a SwitchProbe device or other Remote Monitoring (RMON) probe.

`monitor session`

This command configures a probe port and a monitored port for monitor session (port monitoring). Use the *`source interface <slot/port>`* parameter to specify the interface to monitor. Use *`rx`* to monitor only ingress packets, or use *`tx`* to monitor only egress packets. If you do not specify an *`{rx | tx}`* option, the destination port monitors both ingress and egress packets. Use the *`destination interface <slot/port>`* to specify the interface to receive the monitored traffic. Use the *`mode`* parameter to enabled the administrative mode of the session. If enabled, the probe port monitors all the traffic received and transmitted on the physical monitored port.

Format	**`monitor session`** *`<session-id> {source interface <slot/port> [{rx	tx}]	destination interface <slot/port>	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 <slot/port>`* parameter or *`destination interface <slot/port>`* to remove the specified interface from the port monitoring session. Use the *`mode`* parameter to disable the administrative mode of the session.

Note – Since the current version of FASTPATH only supports one session, if you do not supply optional parameters, the behavior of this command is similar to the behavior of the **`no monitor`** command.

Format	**`no monitor session`** *`<session-id> [{source interface <slot/port> | destination interface <slot/port> | mode}]`*
Mode	Global Config

no monitor

This command removes all the source ports and a destination port for the and restores the default value for mirroring session mode for all the configured sessions.

Note – This is a stand-alone "no" command. This command does not have a "normal" form.

Default	enabled
Format	**`no monitor`**
Mode	Global Config

show monitor session

This command displays the Port monitoring information for a particular mirroring session.

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 one (1).

Format	**`show monitor session`** *`<session-id>`*
Mode	Privileged EXEC

TABLE 3-30 Entry Definitions for `show monitor session`

Entry	Definition
Session ID	An integer value used to identify the session. Its value can be anything between 1 and the maximum number of mirroring sessions allowed on the platform.
Monitor Session Mode	Indicates whether the Port Mirroring feature is enabled or disabled for the session identified with <session-id>. The possible values are Enabled and Disabled.
Probe Port	Probe port (destination port) for the session identified with <*session-id*>. If probe port is not set then this field is blank.
Source Port	The port, which is configured as mirrored port (source port) for the session identified with <session-id>. If no source port is configured for the session then this field is blank.
Type	Direction in which source port configured for port mirroring.Types are tx for transmitted packets and rx for receiving packets.

Static MAC Filtering

The commands in this section describe how to configure static MAC filtering.

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 as follows:

- 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
- FF:FF:FF:FF:FF:FF.

The *<vlanid>* parameter must identify a valid VLAN. You can create up to 100 static MAC filters.

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 addsrc

This command adds the interface 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 select *<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

TABLE 3-31 Entry Definitions for `show mac-address-table static`

Entry	Definition
MAC Address	Is the MAC Address of the static MAC filter entry.
VLAN ID	Is the VLAN ID of the static MAC filter entry.
Source Port(s)	Indicates the source port filter set's slot and port(s).

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

TABLE 3-32 Entry Definitions for `show mac-address-table staticfiltering`

Entry	Definition
Mac Address	A unicast MAC address for which the switch has forwarding and or filtering information. The format is 6 or 8 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB. In an IVL system the MAC address will be displayed as 8 bytes.
Type	Displays the type of the entry. Static entries are those that are configured by the end user. Dynamic entries are added to the table as a result of a learning process or protocol.
Description	The text description of this multicast table entry.
Interfaces	The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).

IGMP Snooping Configuration Commands

This section describes the commands you use to configure IGMP snooping. FASTPATH 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.

`set igmp`

This command enables IGMP Snooping on the system (Global Config Mode) or an interface (Interface Config Mode). This command also enables IGMP snooping on a particular VLAN 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`** *`<vlanid>`*
Modes	Global Config Interface Config VLAN Mode

no set igmp

This command disables IGMP Snooping on the system.

Format	**`no set igmp`** *`<vlanid>`*
Modes	Global Config Interface Config VLAN Mode

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 or 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.

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`** *`<vlanid>`*
Modes	Interface Config VLAN Mode

no set igmp fast-leave

This command disables IGMP Snooping fast-leave admin mode on a selected interface.

Format	**`no set igmp fast-leave`** *`<vlanid>`*
Modes	Interface Config VLAN Mode

set igmp groupmembership-interval

This command sets the IGMP 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 IGMPv3 Maximum Response time value. The range is 2 to 3600 seconds.

Default	260 seconds
Format	**`set igmp groupmembership-interval`** *`<vlanid> <2-3600>`*
Modes	Interface Config Global Config VLAN Mode

no set igmp groupmembership-interval

This command sets the IGMPv3 Group Membership Interval time to the default value.

Format	**`no set igmp groupmembership-interval`**
Modes	Interface Config Global Config VLAN Mode

set igmp maxresponse

This command sets the IGMP 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 IGMP Query Interval time value. The range is 1 to 3599 seconds.

Default	10 seconds
Format	**`set igmp maxresponse`** *<1-3599>*
Modes	Global Config Interface Config VLAN Mode

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`**
Modes	Global Config Interface Config VLAN Mode

set igmp mcrtexpiretime

This command sets 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 time-out, i.e. no expiration.

Default	0
Format	**`set igmp mcrtexpiretime`** *`<vlanid> <0-3600>`*
Modes	Global Config Interface Config

no set igmp mcrtexpiretime

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 mcrtexpiretime`** *`<vlanid>`*
Modes	Global Config
Interface Config	

set igmp mrouter

This command configures the VLAN ID for the VLAN that has the multicast router mode enabled.

Format	**`set igmp mrouter <`***`vlanid`***`>`**
Mode	Interface Config

no set igmp mrouter

This command disables multicast router mode for a VLAN with a particular VLAN ID.

Format	**`no set igmp mrouter`** `<`*`vlanid`*`>`
Mode	Interface Config

set igmp mrouter interface

This command configures the interface 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

show igmpsnooping

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

Format	**`show igmpsnooping`** *`[<slot/port>	<vlanid>]`*
Mode	Privileged EXEC

When the optional arguments *<slot/port>* or *<vlanid>* are not used, the command displays the following information.

TABLE 3-33 Entry Definitions for `show igmpsnooping`

Entry	**Definition**
Admin Mode	This indicates whether or not IGMP Snooping is active on the switch.
Interfaces Enabled for IGMP Snooping	Interfaces on which IGMP Snooping is enabled.
Multicast Control Frame Count	This displays the number of multicast control frames that are processed by the CPU.
VLANS Enabled for IGMP Snooping	VLANS on which IGMP Snooping is enabled.

When you specify the *<slot/port>* values, the following information displays.

TABLE 3-34 Entry Definitions for `show igmpsnooping <slot/port>`

Entry	**Definition**
IGMP Snooping Admin Mode	ndicates whether IGMP Snooping is active on the interface.
Fast Leave Mode	Indicates whether IGMP 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 additional information appears.

VLAN Admin Mode	Indicates whether IGMP Snooping is active on the VLAN.

`show igmpsnooping mrouter interface`

This command displays information about statically configured ports.

Format	**`show igmpsnooping mrouter interface`** *`<slot/port>`*
Mode	Privileged EXEC

TABLE 3-35 Entry Definitions for `show igmpsnooping mrouter interface`

Entry	Definition
Interface	Shows the port on which multicast router information is being displayed.
Multicast Router Attached	Indicates whether multicast router is statically enabled on the interface.
VLAN ID	Displays 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`** *`<slot/port>`*
Mode	Privileged EXEC

TABLE 3-36 Entry Definitions for `show igmpsnooping mrouter vlan`

Entry	Definition
Interface	Shows the port on which multicast router information is being displayed.
VLAN ID	Displays 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

TABLE 3-37 Entry Definitions for `show mac-address-table igmpsnooping`

Entry	Definition
MAC Address	A multicast MAC address for which the switch has forwarding or filtering information. The format is two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB. In an IVL system the MAC address is displayed as a MAC address and VLAN ID combination of 8 bytes.
Type	Displays 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:).

Port Security Commands

This section describes the command you use to configure Port Security on the switch. Port security, which is also known as port MAC locking, allows you to secure the network by locking allowable MAC addresses on a given port. Packets with a matching source MAC address are forwarded normally, and all other packets are discarded.

Note – To enable the SNMP trap specific to port security, see "snmp-server enable traps violation" on page 506.

`port-security`

This command enables port locking at the system level (Global Config) or port level (Interface Config)

Default	disabled
Format	**`port-security`**
Modes	Global Config Interface Config

no port-security

This command disables port locking at the system level (Global Config) or port level (Interface Config).

Format	**`no port-security`**
Modes	Global Config Interface Config

port-security max-dynamic

This command sets the maximum of dynamically locked MAC addresses allowed on a specific port.

Default	600
Format	**`port-security max-dynamic`** *`<maxvalue>`*
Mode	Interface Config

no port-security max-dynamic

This command resets the maximum 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 specific port.

Default	20
Format	**`port-security max-static`** *`<maxvalue>`*
Mode	Interface Config

no port-security max-static

This command resets the maximum of statically locked MAC addresses allowed on a specific port to its 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. 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.

Format	**`port-security mac-address move`**
Mode	Interface Config

`show port-security`

This command displays the port-security settings. If you do not use a parameter, the command displays the settings for the entire system. Use the optional parameters to display the settings on a specific interface or on all interfaces.

Format	**`show port-security`** *`[{<slot/port>	all}]`*
Mode	Privileged EXEC

For each interface, or for the interface you specify, the following information appears.

TABLE 0-4 Entry Definitions for `show port-security`

Entry	Definition
Admin Mode	Port Locking mode for the Interface. This field displays if you do not supply any parameters.
Dynamic Limit	Maximum dynamically allocated MAC Addresses.
Static Limit	Maximum statically allocated MAC Addresses.
Violation Trap Mode	Whether violation traps are enabled.

`show port-security dynamic`

This command displays the dynamically locked MAC addresses for the port.

Format	**`show port-security dynamic`** *`<slot/port>`*
Mode	Privileged EXEC
MAC Address	MAC Address of dynamically locked MAC.

show port-security static

This command displays the statically locked MAC addresses for port.

Format	**`show port-security static`** *`<slot/port>`*
Mode	Privileged EXEC
MAC Address	MAC Address of statically locked MAC.

show port-security violation

This command displays the source MAC address of the last packet discarded on a locked port.

Format	**`show port-security violation`** *`<slot/port>`*
Mode	Privileged EXEC
MAC Address	MAC Address of discarded packet on locked port.

LLDP (802.1AB) Commands

This section describes the command you use to configure Link Layer Discovery Protocol (LLDP), which is defined in the IEEE 802.1AB specification. LLDP allows stations on an 802 LAN to advertise major capabilities and physical descriptions. The advertisements allow a network management system (NMS) to access and display this information.

lldp transmit

Use this command to enable the LLDP advertise capability.

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.

Default	disabled
Format	**`lldp receive`**
Mode	Interface Configuration

no lldp receive

Use this command to return the reception of LLDPDUs to the default value.

Format	**`lldp receive`**
Mode	Interface Configuration

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 re-initialization, 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. Use *sys-name* to transmit the system name TLV. To configure the system name, see See "snmp-server" on page 502. 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 See "description" on page 31.

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.

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.

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.

Format	**`clear lldp statistics`**
Mode	Global Config

clear lldp remote-data

Use this command to delete all information from the LLDP remote data table.

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

TABLE 3-38 Entry Defintions for `show lldp`

Entry	Definition
Transmit Interval	Shows how frequently the system transmits local data LLDPDUs, in seconds.
Transmit Hold Multiplier	Shows the multiplier on the transmit interval that sets the TTL in local data LLDPDUs.
Re-initialization Delay	Shows the delay before re-initialization, in seconds.
Notification Interval	Shows how frequently the system sends remote data change notifications, in seconds.

show lldp interface

Use this command to display a summary of the current LLDP configuration for a specific interface or for all interfaces.

Format	**`show lldp interface`** *`{<slot/port>	all}`*
Mode	Privileged EXEC

TABLE 3-39 Entry Defintions for `show lldp interface`

Entry	Definition
Interface	Shows the interface in a slot/port format.
Link	Shows whether the link is up or down.
Transmit	Shows whether the interface transmits LLDPDUs.
Receive	Shows whether the interface receives LLDPDUs.
Notify	Shows whether the interface sends remote data change notifications.
TLVs	Shows whether the interface sends optional TLVs in the LLDPDUs. The TLV codes can be 0 (Port Description), 1 (System Name), 2 (System Description), or 3 (System Capability).
Mgmt	Shows whether the interface transmits system management address information in the LLDPDUs.

show lldp statistics

Use this command to display the current LLDP traffic and remote table statistics for a specific interface or for all interfaces.

Format	**`show lldp statistics`** *`{<slot/port> | all}`*
Mode	Privileged EXEC

TABLE 3-40 Entry Definitions for `show lldp statistics`

Entry	Definition
Last Update	Shows 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 headings.
Interface	Shows the interface in slot/port format.
Transmit Total	Total number of LLDP packets transmitted on the port.
Receive Total	Total number of LLDP packets received on the port.

TABLE 3-40 Entry Definitions for `show lldp statistics`

Entry	Definition
Errors	The number of invalid LLDP frames received on the port.
Ageouts	Total number of times a complete remote data entry was deleted for the port because the Time to Live interval expired.
TVL Discards	Shows 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.

show lldp remote-device

Use this command to display summary information about remote devices that transmit current LLDP data to the system. You can show information about LLDP remote data received on all ports or on a specific port.

Format	**`show lldp remote-device`** ***`{<slot/port>	all}`***
Mode	Privileged EXEC

TABLE 3-41 Entry Definitions for `show lldp remote-device`

Entry	Definition
Local Interface	Identifies the interface that received the LLDPDU from the remote device.
Chassis ID	Shows the ID of the remote device.
Port ID	Shows the port number that transmitted the LLDPDU.
System Name	Shows the system name of the remote device.

show lldp remote-device detail

Use this command to display detailed information about remote devices that transmit current LLDP data to an interface on the system.

Format	**`show lldp remote-device detail`** *`<slot/port>`*
Mode	Privileged EXEC

TABLE 3-42 Entry Definitions for `show lldp remote-device detail`

Entry	Definition
Local Interface	Identifies the interface that received the LLDPDU from the remote device.
Chassis ID Subtype	Shows the type of identification used in the Chassis ID field.
Chassis ID	Identifies the chassis of the remote device.
Port ID Subtype	Identifies the type of port on the remote device.
Port ID	Shows the port number that transmitted the LLDPDU.
System Name	Shows the system name of the remote device.
System Description	Describes the remote system by identifying the system name and versions of hardware, operating system, and networking software supported in the device.
Port Description	Describes the port in an alpha-numeric format. The port description is configurable.
System Capabilities Supported	Indicates the primary function(s) of the device.
System Capabilities Enabled	Shows which of the supported system capabilities are enabled.
Management Address	For each interface on the remote device with an LLDP agent, lists the type of address the remote LLDP agent uses and specifies the address used to obtain information related to the device.
Time To Live	Shows the amount of time (in seconds) the remote device's information received in the LLDPDU should be treated as valid information.

show lldp local-device

Use this command to display summary information about the advertised LLDP local data. This command can display summary information or detail for each interface.

Format	**`show lldp local-device`** *{<slot/port> | all}*
Mode	Privileged EXEC

TABLE 3-43 Entry Definitions for `show lldp local-device`

Entry	Definition
Interface	Identifies the interface in a slot/port format.
Port ID	Shows the port ID associated with this interface.
Port Description	Shows the port description associated with the interface.

`show lldp local-device detail`

Use this command to display detailed information about the LLDP data a specific interface transmits.

Format	**`show lldp local-device detail`** *<slot/port>*
Mode	Privileged EXEC

TABLE 3-44 Entry Definitions for `show lldp local-device detail`

Entry	Definition
Interface	Identifies the interface that sends the LLDPDU.
Chassis ID Subtype	Shows the type of identification used in the Chassis ID field.
Chassis ID	Identifies the chassis of the local device.
Port ID Subtype	Identifies the type of port on the local device.
Port ID	Shows the port number that transmitted the LLDPDU.
System Name	Shows the system name of the local device.
System Description	Describes the local system by identifying the system name and versions of hardware, operating system, and networking software supported in the device.
Port Description	Describes the port in an alpha-numeric format.
System Capabilities Supported	Indicates the primary function(s) of the device.
System Capabilities Enabled	Shows which of the supported system capabilities are enabled.
Management Address	Lists the type of address and the specific address the local LLDP agent uses to send and receive information.

Denial of Service Commands

This section describes the commands you use to configure DoS Control. FASTPATH software provides support for classifying and blocking specific types of Denial of Service attacks.

You can configure your system to monitor and block six types of attacks:

1. SIP=DIP: Source IP address = Destination IP address.
2. First Fragment:TCP Header size smaller then configured value.
3. TCP Fragment: IP Fragment Offset = 1.
4. 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.
5. L4 Port: Source TCP/UDP Port = Destination TCP/UDP Port.
6. ICMP: Limiting the size of ICMP Ping packets.

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. If packets ingress having IP Fragment Offset equal to one (1), the packets will be dropped if the mode is enabled.

Default	disabled
Format	**`dos-control tcpfrag`**
Mode	Global Config

no dos-control tcpfrag

This command disabled TCP Fragment Denial of Service protection.

Format	**`no storm-control broadcast all`**
Mode	Global Config

dos-control tcpflag

This command enables TCP Flag Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attacks. If packets ingress having TCP Flag SYN set and a source port less than 1024 or having TCP Control Flags set to 0 and TCP Sequence Number set to 0 or having TCP Flags FIN, URG, and PSH set and TCP Sequence Number set to 0 or having TCP Flags SYN and FIN both set, the packets will be dropped if the mode is enabled.

Default	disabled
Format	**`dos-control tcpflag`**
Mode	Global Config

no dos-control tcpflag

This command sets disables TCP Flag Denial of Service protections.

Format	**`no dos-control tcpflag`**
Mode	Global Config

dos-control l4port

This command enables L4 Port Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having Source TCP/UDP Port Number equal to Destination TCP/UDP Port Number, the packets will be dropped if the mode is enabled.

Note – Some applications mirror source and destination L4 ports - RIP for example uses 520 for both. If you enable dos-control l4port, applications such as RIP may experience packet loss which would render the application inoperable.

Default	disabled
Format	**`dos-control l4port`**
Mode	Global Config

no dos-control l4port

This command disables L4 Port Denial of Service protections.

Format	**`no dos-control l4port`**
Mode	Global Config

dos-control icmp

This command enables Maximum ICMP Packet Size Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attack. If ICMP Echo Request (PING) packets ingress having a size greater than the configured value, the packets will be dropped if the mode is enabled.

Default	disabled <512>
Format	**`dos-control icmp`** *`<0-1023>`*
Mode	Global Config

no dos-control icmp

This command disables Maximum ICMP Packet Size Denial of Service protections.

Format	**`no dos-control icmp`**
Mode	Global Config

show dos-control

This command displays Denial of Service configuration information.

Format	**`show dos-control`**
Mode	Privileged EXEC

TABLE 3-45 Entry Definitions for `show dos-control`

Entry	Definition
SIPDIP Mode	May be enabled or disabled. The factory default is disabled.
First Fragment Mode	May be enabled or disabled. The factory default is disabled.
Min TCP Hdr Size <0-255>	The factory default is 20.
TCP Fragment Mode	May be enabled or disabled. The factory default is disabled.
TCP Flag Mode	May be enabled or disabled. The factory default is disabled.

TABLE 3-45 Entry Definitions for `show dos-control`

Entry	Definition
L4 Port Mode	May be enabled or disabled. The factory default is disabled.
ICMP Mode	May be enabled or disabled. The factory default is disabled.
Max ICMP Pkt Size <0-1023>	The factory default is 512.

MAC Database Commands

This section describes the commands you use to configure and view information about the MAC databases.

`bridge aging-time`

This command configures the forwarding database address aging timeout in seconds. The *`<seconds>`* parameter must be within the range of 10 to 1,000,000 seconds.

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.

Format	**`no bridge aging-time`**
Mode	Global Config

show forwardingdb agetime

This command displays the timeout for address aging. In an IVL system, the [fdbid | all] parameter is required.

Default	all
Format	**`show forwardingdb agetime`** *`[fdbid	all]`*
Mode	Privileged EXEC

TABLE 3-46 Entry Definitions for `show forwardingdb agetime`

Entry	Definition
Forwarding DB ID	Fdbid (Forwarding database ID) indicates the forwarding database whose aging timeout is to be shown. The all option is used to display the aging timeouts associated with all forwarding databases. This field displays the forwarding database ID in an IVL system.
Agetime	In an IVL system, this parameter displays the address aging timeout for the associated forwarding database.

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

TABLE 3-47 Entry Definitions for `show mac-address-table multicast`

Entry	Definition
MAC Address	A multicast MAC address for which the switch has forwarding and or filtering information. The format is two-digit hexadecimal numbers separated by colons, for example 01:23:45:67:89:AB. In an IVL system the MAC address will be displayed as a MAC address and VLAN ID combination of 8 bytes.
Type	This displays the type of the entry. Static entries are those that are configured by the end user. Dynamic entries are added to the table as a result of a learning process or protocol.
Component	The component that is responsible for this entry in the Multicast Forwarding Database. Possible values are IGMP Snooping, GMRP, and Static Filtering.
Description	The text description of this multicast table entry.
Interfaces	The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).
Forwarding Interfaces	The resultant forwarding list is derived from combining all the component's forwarding interfaces and removing the interfaces that are listed as the static filtering interfaces.

show mac-address-table stats

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

Format	**`show mac-address-table stats`**
Mode	Privileged EXEC

TABLE 3-48 Entry Definitions for `show mac-address-table stats`

Entry	Definition
Total Entries	Displays the total number of entries that can possibly be in the Multicast Forwarding Database table.
Most MFDB Entries Ever Used	Displays the largest number of entries that have been present in the Multicast Forwarding Database table. This value is also known as the MFDB high-water mark.
Current Entries	Displays the current number of entries in the MFDB

Layer 2 Failover Commands

This section describes the Layer 2 failover commands. Layer 2 failover functionality disables configured server ports in case a monitored uplink port or port channel fails. This failover is designed to be used with NIC teaming or bonding to facilitate uplink redundancy without the need for Layer 2 connections between Fabric/Base switches.

Layer 2 failover incorparates the track object features of VRRP, using the object status to determine uplink status to the switch. For commands and configuration guidelines, see "VRRP Tracking Commands" on page 194.

failover track

This command configures the interface to track the configured monitor and to disable the interface if the monitor status is down. The number at the end of the command corresponds to the track object number listed under the global configuration.

Default	disabled
Format	**`Failover track`** `[ <1-255> ]`
Mode	Interface Config

show track failover

Show status of single or all interfaces configured with the failover track command.

Format	**`show track failover`** `[ interface <0/#> ] [all]`
Mode	Privileged EXEC

TABLE 3-49 Entry Definitions for `show track failover`

Entry	Definition
Interface	Displays interfaces configured with failover track command.

TABLE 3-49 Entry Definitions for `show track failover`

Entry	Definition
Track Num	Displays the tracking object number associated with the listed interface.
Track Status	Displays the status of the tracking object (up or down).
Interface Status	Displays the status of the interface configured with the failover track command. • Up indicates the tracked object is up and the interface is connected and active. • Disabled indicates the tracked object is down and the interface link state has been disabled.

Link Aggregation (LAG)/Port-Channel (802.3AD) Commands

This section provides a detailed explanation of the link aggregation (LAG) commands. The commands are divided into 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.

`port-channel staticcapability`

This command enables the support of port-channels (static link aggregations - LAGs) on the device. By default, the static capability for all port-channels is disabled.

- Default – disabled
- Format – `port-channel staticcapability`
- Mode – Global Config

`no port-channel staticcapability`

This command disables the support of static port-channels (link aggregations - LAGs) on the device.

- Format – `no port-channel staticcapability`

- Mode – Global Config

port lacpmode

This command enables Link Aggregation Control Protocol (LACP) on a port.

- Default – disabled
- 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 all

This command enables Link Aggregation Control Protocol (LACP) on all ports.

- Format – `port lacpmode all`
- Mode – Global Config

no port lacpmode all

This command disables Link Aggregation Control Protocol (LACP) on all ports.

- Format – `no port lacpmode all`
- Mode – Global Config

port-channel

This command configures a new port-channel (LAG) and generates a logical slot/port number for the port-channel. The <name> field is a character string which allows the dash '-' character as well as alphanumeric characters. Display this number using the “show port-channel”.

Note – Before including a port in a port-channel, set the port physical mode (see "speed" on page 34).

- Format – `port-channel <name>`
- Mode – Global Config

no port-channel

This command deletes a port-channel (LAG).

- Format – `no port-channel <name>`
- Mode – Global Config

port-channel adminmode all

This command enables a port-channel (LAG). The interface is a logical slot/port for a configured port-channel. The option `all` sets every configured port-channel with the same administrative mode setting.

- Format – `port-channel adminmode all`
- Mode – Global Config

no port-channel adminmode

This command disables a port-channel (LAG). The interface is a logical slot/port for a configured port- channel. The option `all sets` every configured port-channel with the same administrative mode setting.

- Format – `no port-channel adminmode all`
- Mode – Global Config

port-channel linktrap

This command enables link trap notifications for the port-channel (LAG). The interface is a logical slot/ port for a configured port-channel. The option `all` sets every configured port-channel with the same administrative mode setting.

- Default – enabled
- Format – `port-channel linktrap {<logical slot/port> | all}`
- Mode – Global Config

`no port-channel linktrap`

This command disables link trap notifications for the port-channel (LAG). The interface is a logical unit, slot and port slot and port for a configured port-channel. The option all sets every configured port-channel with the same administrative mode setting.

- Format – `no port-channel linktrap {<logical slot/port> | all]`
- Mode – GlobalConfig

`port-channel name`

This command defines a name for the port-channel (LAG). The interface is a logical slot/port for a configured port-channel, and name is an alphanumeric string up to 15 characters. This command is used to modify the name that was associated with the port-channel when it was created.

- Format – `port-channel name {<logical slot/port> | all | <name>}`
- Mode – Global Config

`show port-channel brief`

This command displays the static capability of all port-channels (LAGs) on the device as well as a summary of individual port-channels.

- Format – `show port-channel brief`
- Mode – Privileged EXEC and User EXEC

TABLE 3-50 Entry Definitions for `show port-channel brief`

Entry	**Definition**
Static Capability	This field displays whether or not the device has static capability enabled.

For each port-channel, the following information is displayed.

TABLE 3-51 Informaiton Displayed For Each Channel of `show port-channel brief`

Entry	Definition
Name	This field displays the name of the port-channel.
Link State	This field indicates whether the link is up or down.
Mbr Ports	This field lists the ports that are members of this port-channel, in <slot/port> notation.
Active Ports	This field lists the ports that are actively participating in this port-channel.

show port-channel

This command displays an overview of all port-channels (LAGs) on the switch.

- Format – `show port-channel {<logical slot/port> | all}`
- Mode – `Privileged EXEC`

TABLE 3-52 Entry Definitions for `show port-channel`

Entry	Definition
Logical slot/port	Valid slot and port number separated by forward slashes.
Name	The name of this port-channel (LAG). You may enter any string of up to 15 alphanumeric characters.
Link State	Indicates whether the Link is up or down.
Admin Mode	May be enabled or disabled. The factory default is enabled.
Link Trap Mode	This object determines whether or not to send a trap when link status changes. The factory default is enabled.
STP Mode	The Spanning Tree Protocol Administrative Mode associated with the port or port-channel (LAG). The possible values are: • Disable – Spanning tree is disabled for this port. • Enable – Spanning tree is enabled for this port.
Mbr Ports	A listing of the ports that are members of this port-channel (LAG), in slot/port notation. There can be a maximum of eight ports assigned to a given port-channel (LAG).

TABLE 3-52 Entry Definitions for `show port-channel`

Entry	Definition
Port Speed	Speed of the port-channel port.
Type	This field displays the status designating whether a particular port-channel (LAG) is statically or dynamically maintained. The possible values of this field are: • Static, indicating that the port-channel is statically maintained • Dynamic, indicating that the port-channel is dynamically maintained.
Active Ports	This field lists the ports that are actively participating in the port-channel (LAG).

CHAPTER 4

Routing Commands

This chapter describes the routing commands available in the FASTPATH® CLI.

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

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

This chapter contains the following sections:

Address Resolution Protocol (ARP) Commands

This section describes the commands you use to configure ARP and to view ARP information on the switch. ARP associates IP addresses with MAC addresses and stores the information as ARP entries in the ARP cache.

`arp`

This command creates an ARP entry. The value for *`<ipaddress>`* is the IP address of a device on a subnet attached to an existing routing interface. *`<macaddr>`* is a unicast MAC address for that device.

The format is 6 two-digit hexadecimal numbers that are separated by colons, for example 00:06:29:32:81:40.

Format	**`arp`** *`<ipaddress> <macaddr>`*
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. *`<macaddr>`* is a unicast MAC address for that device.

Format	**`no arp`** *`<ipaddress> <macaddr>`*
Mode	Global Config

`ip proxy-arp`

This command enables proxy ARP on a router interface. 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

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.

Default	enabled
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`** *`<ipaddr>`*
Mode	Privileged EXEC

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

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

TABLE 4-1 Entry Definitions for `show arp`

Entry	**Definition**
Age Time (seconds)	Is the time it takes for an ARP entry to age out. This value was configured into the unit. Age time is measured in seconds.
Response Time (seconds)	Is the time it takes for an ARP request timeout. This value was configured into the unit. Response time is measured in seconds.
Retries	Is the maximum number of times an ARP request is retried. This value was configured into the unit.
Cache Size	Is the maximum number of entries in the ARP table. This value was configured into the unit.

TABLE 4-1 Entry Definitions for `show arp` *(Continued)*

Entry	Definition
Dynamic Renew Mode	Displays whether the ARP component automatically attempts to renew dynamic ARP entries when they age out.
Total Entry Count Current / Peak	Field listing the total entries in the ARP table and the peak entry count in the ARP table.
Static Entry Count Current / Max	Field listing the static entry count in the ARP table and maximum static entry count in the ARP table. The following entries are displayed for each ARP entry.
IP Address	Is the IP address of a device on a subnet attached to an existing routing interface.
MAC Address	Is the hardware MAC address of that device.
Interface	Is the routing slot/port associated with the device ARP entry.
Type	Is the type that was configured into the unit. The possible values are Local, Gateway, Dynamic and Static.
Age	This field displays 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

TABLE 4-2 Entry Definitions for `show arp brief`

Entry	Definition
Age Time (seconds)	Is the time it takes for an ARP entry to age out. This value was configured into the unit. Age time is measured in seconds.
Response Time (seconds)	Is the time it takes for an ARP request timeout. This value was configured into the unit. Response time is measured in seconds.
Retries	Is the maximum number of times an ARP request is retried. This value was configured into the unit.
Cache Size	Is the maximum number of entries in the ARP table. This value was configured into the unit.

TABLE 4-2 Entry Definitions for `show arp brief` *(Continued)*

Entry	Definition
Dynamic Renew Mode	Displays whether the ARP component automatically attempts to renew dynamic ARP entries when they age out.
Total Entry Count Current / Peak	Field listing the total entries in the ARP table and the peak entry count in the ARP table.
Static Entry Count Current / Max	Field listing 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

TABLE 4-3 Entry Definitions for `show arp switch`

Entry	Definition
IP Address	Is the IP address of a device on a subnet attached to the switch.
MAC Address	Is the hardware MAC address of that device.
Interface	Is the routing slot/port associated with the device's ARP entry.

IP Routing Commands

This section describes the commands you use to enable and configure IP routing on the switch.

`routing`

This command enables IPv4 and IPv6 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.”

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

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. You can also use this command to configure one or more secondary IP addresses on the interface.The value for *<ipaddr>* is the IP Address of the interface. The value for *<subnetmask>* is a 4-digit dotted-decimal number which represents the subnet mask of the interface. The subnet mask must have contiguous ones and be no longer than 30 bits, for example 255.255.255.0. This command changes the label IP address in **`show ip interface`**.

Format	**`ip address`** *`<ipaddr> <subnetmask> [secondary]`*
Mode	Interface Config

no ip address

This command deletes an IP address from an interface. The value for *<ipaddr>* is the IP Address of the interface. The value for *<subnetmask>* is a 4-digit dotted-decimal number which represents the Subnet Mask of the interface.

Format	**`no ip address`** *`<ipaddr> <subnetmask> [secondary]`*
Mode	Interface 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.

- 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.

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> [<preference>]`*
Mode	Global Config

no ip route

This command deletes all next hops 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>}]`*
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 forwarding

This command enables forwarding of IP frames.

Default	enabled
Format	**`ip forwarding`**
Mode	Global Config

no ip forwarding

This command disables forwarding of IP frames.

Format	**`no ip forwarding`**
Mode	Global Config

ip netdirbcast

This command enables the forwarding of network-directed broadcasts. 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. The IP MTU is the size of the largest IP packet that can be transmitted on the interface without fragmentation. FASTPATH software currently does not fragment IP packets.

- Packets forwarded in hardware ignore the IP MTU.
- Packets forwarded in software are dropped if they exceed the IP MTU of the outgoing interface.

Packets originated on the router, such as OSPF packets, may be fragmented by the IP stack. The IP stack uses its default IP MTU and ignores the value set using the ip mtu command.

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 32.) must take into account the size of the Ethernet header.

Default	1500 bytes
Format	**`ip mtu`** *`<68-1500>`*
Mode	Interface Config

`no ip mtu`

This command resets the ip mtu to the default value.

Format	**`no ip mtu`** *`<mtu>`*
Mode	Interface Config

`encapsulation`

This command configures the link layer encapsulation type for the packet. 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 ip brief`

This command displays all the summary information of the IP.

Format	**`show ip brief`**
Modes	Privileged EXEC User EXEC

TABLE 4-4 Entry Definitions for `show ip brief`

Entry	**Definition**
Default Time to Live	The computed TTL (Time to Live) of forwarding a packet from the local router to the final destination.

TABLE 4-4 Entry Definitions for `show ip brief`

Entry	Definition
Routing Mode	Shows whether the routing mode is enabled or disabled.
IP Forwarding Mode	Shows whether forwarding of IP frames is enabled or disabled. This is a configured value.
Maximum Next Hops	Shows the maximum number of next hops the packet can travel.

`show ip interface`

This command displays all pertinent information about the IP interface.

Format	**`show ip interface`** *`<slot/port>`*
Modes	Privileged EXEC User EXEC

TABLE 4-5 Entry Definitions for `show ip interface`

Entry	Definition
Primary IP Address	Displays the primary IP address and subnet masks for the interface. This value appears only if you configure it.
Secondary IP Address	Displays one or more secondary IP addresses and subnet masks for the interface. This value appears only if you configure it.
Routing Mode	Is the administrative mode of router interface participation. The possible values are enable or disable. This value was configured into the unit.
Administrative Mode	Is the administrative mode of the specified interface. The possible values of this field are enable or disable. This value was configured into the unit.
Forward Net Directed Broadcasts	Displays whether forwarding of network-directed broadcasts is enabled or disabled. This value was configured into the unit.
Proxy ARP	Displays whether Proxy ARP is enabled or disabled on the system.
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	Is an integer representing the physical link data rate of the specified interface. This is measured in Megabits per second (Mbps).

TABLE 4-5 Entry Definitions for `show ip interface`

Entry	Definition
MAC Address	Is the burned in physical address of the specified interface. The format is 6 two-digit hexadecimal numbers that are separated by colons.
Encapsulation Type	Is the encapsulation type for the specified interface. The types are: Ethernet or SNAP.
IP MTU	Displays the maximum transmission unit (MTU) size of a frame, in bytes.

`show ip interface brief`

This command displays summary information about IP configuration settings for all ports in the router.

Format	**`show ip interface brief`**
Modes	Privileged EXEC User EXEC

TABLE 4-6 Entry Definitions for `show ip interface brief`

Entry	Definition
Interface	Valid slot and port number separated by forward slashes.
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.
Netdir Bcast	Indicates if IP forwards net-directed broadcasts on this interface. Possible values are Enable or Disable.
MultiCast Fwd	Indicates the multicast forwarding administrative mode on the interface. Possible values are Enable or Disable.

`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*, *static*, or *bgp*.
- Use the *all* parameter to display all routes including best and non-best routes. If you do not use the *all* parameter, the command only displays the best route.

Note – If you use the *connected* keyword for *<protocol>*, the *all* option is not available because there are no best or non-best connected routes.

Format	**show ip route** *[{<ip-address> [<protocol>] | {<ip-address> <mask> [longer-prefixes] [<protocol>] | <protocol>} [all] | all}]*
Mode	Privileged EXEC User EXEC
Route Codes	Displays 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, Interface
```

The columns for the routing table display the following information.

TABLE 4-7 Entry Definitions for `show ip route`

Entry	Definition
Code	The codes for the routing protocols that created the routes.
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
Interface	The outgoing router interface to use when forwarding traffic to the next destination

`show ip route summary`

Use this command to display the routing table summary. Use the optional *`all`* parameter to show the number of all routes, including best and non-best routes. To include only the number of best routes, do not use the optional parameter.

Format	**`show ip route summary`** *`[all]`*
Mode	Privileged EXEC User EXEC

TABLE 4-8 Entry Definitions for `show ip route summary`

Entry	**Definition**
Connected Routes	The total number of connected routes in the routing table.
Static Routes	Total number of static routes in the routing table.
RIP Routes	Total number of routes installed by RIP protocol.
BGP Routes	Total number of routes installed by BGP protocol.
OSPF Routes	Total number of routes installed by OSPF protocol.
Total Routes	Total number of routes in the routing table.

`show ip route preferences`

This command displays detailed information about the route preferences. 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

TABLE 4-9 Entry Definitions for `show ip route preferences`

Entry	**Definition**
Local	This field displays the local route preference value.
Static	This field displays the static route preference value.
OSPF Intra	This field displays the OSPF Intra route preference value.

TABLE 4-9 Entry Definitions for `show ip route preferences`

Entry	Definition
OSPF Inter	This field displays the OSPF Inter route preference value.
OSPF Ext T1	This field displays the OSPF External Type-1 route preference value.
OSPF Ext T2	This field displays the OSPF External Type-2 route preference value.
OSPF NSSA T1	This field displays the OSPF NSSA Type-1 route preference value.
OSPF NSSA T2	This field displays the OSPF NSSA Type-2 route preference value.
RIP	This field displays the RIP route preference value.
BGP4	This field displays the BGP-4 route preference value.

Note – The configuration of NSSA preferences is not supported in this release.

`show ip stats`

This command displays IP statistical information. Refer to RFC 1213 for more information about the fields that are displayed.

Format	**`show ip stats`**
Modes	Privileged EXEC User EXEC

Router Discovery Protocol Commands

This section describes the commands you use to view and configure Router Discovery Protocol settings on the switch. The Router Discovery Protocol enables a host to discover the IP address of routers on the subnet.

`ip irdp`

This command enables Router Discovery on an interface.

Default	disabled
Format	**`ip irdp`**
Mode	Interface Config

`no ip irdp`

This command disables Router Discovery on an interface.

Format	**`no ip irdp`**
Mode	Interface Config

`ip irdp address`

This command configures the address that the interface uses to send the router discovery advertisements. The valid values for *<ipaddr>* are 224.0.0.1, which is the all-hosts IP multicast address, and 255.255.255.255, which is the limited broadcast address.

Default	224.0.0.1
Format	**`ip irdp address`** *<ipaddr>*
Mode	Interface Config

`no ip irdp address`

This command configures the default address used to advertise the router for the interface.

Format	**`no ip irdp address`**
Mode	Interface Config

`ip irdp holdtime`

This command configures the value, in seconds, of the holdtime field of the router advertisement sent from this interface. The holdtime range is the value of *`<maxadvertinterval>`* to 9000 seconds.

Default	3 * maxinterval
Format	**`ip irdp holdtime`** *`<maxadvertinterval-9000>`*
Mode	Interface Config

`no ip irdp holdtime`

This command configures the default value, in seconds, of the holdtime field of the router advertisement sent from this interface.

Format	**`no ip irdp holdtime`**
Mode	Interface Config

`ip irdp maxadvertinterval`

This command configures the maximum time, in seconds, allowed between sending router advertisements from the interface. The range for maxadvertinterval is 4 to 1800 seconds.

Default	600
Format	**`ip irdp maxadvertinterval`** *`<4-1800>`*
Mode	Interface Config

no ip irdp maxadvertinterval

This command configures the default maximum time, in seconds.

Format	**`no ip irdp maxadvertinterval`**
Mode	Interface Config

ip irdp minadvertinterval

This command configures the minimum time, in seconds, allowed between sending router advertisements from the interface. The range for minadvertinterval is three to the value of maxadvertinterval.

Default	0.75 * maxadvertinterval
Format	**`ip irdp minadvertinterval`** *`<3-maxadvertinterval>`*
Mode	Interface Config

no ip irdp minadvertinterval

This command sets the default minimum time to the default.

Format	**`no ip irdp minadvertinterval`**
Mode	Interface Config

ip irdp preference

This command configures the preferability of the address as a default router address, relative to other router addresses on the same subnet.

Default	0
Format	**`ip irdp preference`** *`<-2147483648 to 2147483647>`*
Mode	Interface Config

`no ip irdp preference`

This command configures the default preferability of the address as a default router address, relative to other router addresses on the same subnet.

Format	**`no ip irdp preference`**
Mode	Interface Config

`show ip irdp`

This command displays the router discovery information for all interfaces, or a specified interface.

Format	**`show ip irdp`** *`{<slot/port>	all}`*
Modes	Privileged EXEC User EXEC

TABLE 4-10 Entry Definitions for `show ip irdp`

Entry	**Definition**
Interface	Shows the *`<slot/port>`* that matches the rest of the information in the row.
Ad Mode	Displays the advertise mode, which indicates whether router discovery is enabled or disabled on this interface.
Advertise Address	Displays the IP address to which the interface sends the advertisement.
Max Int	Displays the maximum advertise interval, which is the maximum time, in seconds, allowed between sending router advertisements from the interface.
Min Int	Displays the minimum advertise interval, which is the minimum time, in seconds, allowed between sending router advertisements from the interface.
Hold Time	Displays the amount of time, in seconds, that a system should keep the router advertisement before discarding it.
Preference	Displays the preference of the address as a default router address, relative to other router addresses on the same subnet.

Virtual LAN Routing Commands

This section describes the commands you use to view and configure VLAN routing and to view VLAN routing status information.

`vlan routing`

This command creates routing on a VLAN. The *`<vlanid>`* value has a range from 1 to 4094.

Format	**`vlan routing`** *`<vlanid>`*
Mode	VLAN Config

`no vlan routing`

This command deletes routing on a VLAN. The *`<vlanid>`* value has a range from 1 to 4094.

Format	**`no vlan routing`** *`<vlanid>`*
Mode	VLAN 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

TABLE 4-11 Entry Definitions for `show ip vlan`

Entry	**Definition**
MAC Address used by Routing VLANs	Is the MAC Address associated with the internalbridge-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	Is the identifier of the VLAN.
Logical Interface	Shows the logical slot/port associated with the VLAN routing interface.
IP Address	Displays the IP Address associated with this VLAN.
Subnet Mask	Indicates the subnet mask that is associated with this VLAN.

Virtual Router Redundancy Protocol Commands

This section describes the commands you use to view and configure Virtual Router Redundancy Protocol (VRRP) and to view VRRP status information. VRRP helps provide failover and load balancing when you configure two devices as a VRRP pair.

`ip vrrp`

In Global Config mode, this command enables the administrative mode of VRRP in the router. In Interface Config mode, this command enables the VRRP protocol on an interface. The parameter *`<vrid>`* is the virtual router ID which has an integer value range from 1 to 255.

Default	none
Format	**`ip vrrp`** *`<vrid>`*
Mode	Global Config Interface Config

`no ip vrrp`

In Global Config mode, this command disables the default administrative mode of VRRP in the router. In Interface Config mode, this command disables the VRRP protocol on an interface. This command also removes a virtual router IP address as a secondary IP address on an interface. The virtual Router ID, *`<vrid>`*, is an integer value that ranges from 1 to 255.

Format	**`no ip vrrp`** *`<vrid> <ipaddress> [secondary]`*
Mode	Global Config Interface Config

`ip vrrp mode`

This command enables the virtual router configured on the specified interface. Enabling the status field starts a virtual router. The parameter *`<vrid>`* is the virtual router ID which has an integer value ranging from 1 to 255.

Default	disabled
Format	**`ip vrrp`** *`<vrid>`* **`mode`**
Mode	Interface Config

`no ip vrrp mode`

This command disables the virtual router configured on the specified interface. Disabling the status field stops a virtual router.

Format	**`no ip vrrp`** *`<vrid>`* **`mode`**
Mode	Interface Config

ip vrrp ip

This command sets the virtual router ipaddress value for an interface. The value for *<ipaddr>* is the IP Address which is to be configured on that interface for VRRP. The parameter *<vrid>* is the virtual router ID which has an integer value range from 1 to 255. You can use the optional *[secondary]* parameter to designate the IP address as a secondary IP address.

Default	none
Format	**`ip vrrp`** *`<vrid>`* **`ip`** *`<ipaddr> [secondary]`*
Mode	Interface Config

ip vrrp authentication

This command sets the authorization details value for the virtual router configured on a specified interface. The parameter *{none | simple}* specifies the authorization type for virtual router configured on the specified interface. The parameter *[key]* is optional, it is only required when authorization type is simple text password. The parameter *<vrid>* is the virtual router ID which has an integer value ranges from 1 to 255.

Default	no authorization
Format	**`ip vrrp`** *`<vrid>`* **`authentication`** *`{none	simple <key>}`*
Mode	Interface Config

no ip vrrp authentication

This command sets the default authorization details value for the virtual router configured on a specified interface.

Format	**`no ip vrrp`** *`<vrid>`* **`authentication`**
Mode	Interface Config

ip vrrp preempt

This command sets the preemption mode value for the virtual router configured on a specified interface. The parameter *<vrid>* is the virtual router ID, which is an integer from 1 to 255

Default	enabled
Format	**`ip vrrp`** *`<vrid>`* **`preempt`**
Mode	Interface Config

no ip vrrp preempt

This command sets the default preemption mode value for the virtual router configured on a specified interface.

Format	**`no ip vrrp`** *`<vrid>`* **`preempt`**
Mode	Interface Config

ip vrrp priority

This command sets the priority value for the virtual router configured on a specified interface. The priority of the interface is a priority integer from 1 to 254. The parameter *<vrid>* is the virtual router ID which has an integer value ranges from 1 to 255.

Default	100
Format	**`ip vrrp`** *`<vrid>`* **`priority`** *`<1-254>`*
Mode	Interface Config

no ip vrrp priority

This command sets the default priority value for the virtual router configured on a specified interface.

Format	**`no ip vrrp`** *`<vrid>`* **`priority`**
Mode	Interface Config

ip vrrp timers advertise

This command sets the frequency, in seconds, that an interface on the specified virtual router sends a virtual router advertisement.

Default	1
Format	**`ip vrrp`** *`<vrid>`* **`timers advertise`** *`<1-255>`*
Mode	Interface Config

no ip vrrp timers advertise

This command sets the default virtual router advertisement value for an interface.

Format	**`no ip vrrp`** *`<vrid>`* **`timers advertise`**
Mode	Interface Config

show ip vrrp interface stats

This command displays the statistical information about each virtual router configured on the FASTPATH switch.

Format	**`show ip vrrp interface stats`** *`<slot/port> <vrid>`*
Modes	Privileged EXEC User EXEC

TABLE 4-12 Entry Definitions for `show ip vrrp interface stats`

Entry	**Definition**
Uptime	The time that the virtual router has been up, in days, hours, minutes and seconds.
Protocol	Represents the protocol configured on the interface.
State Transitioned to Master	Represents the total number of times virtual router state has changed to MASTER.
Advertisement Received	Represents the total number of VRRP advertisements received by this virtual router.

TABLE 4-12 Entry Definitions for `show ip vrrp interface stats` *(Continued)*

Entry	Definition
Advertisement Interval Errors	Represents the total number of VRRP advertisements received for which advertisement interval is different than the configured value for this virtual router.
Authentication Failure	Represents the total number of VRRP packets received that don't pass the authentication check.
IP TTL errors	Represents the total number of VRRP packets received by the virtual router with IP TTL (time to live) not equal to 255.
Zero Priority Packets Received	Represents the total number of VRRP packets received by virtual router with a priority of '0'.
Zero Priority Packets Sent	Represents the total number of VRRP packets sent by the virtual router with a priority of '0'.
Invalid Type Packets Received	Represents the total number of VRRP packets received by the virtual router with invalid 'type' field.
Address List Errors	Represents the total number of VRRP packets received for which address list does not match the locally configured list for the virtual router.
Invalid Authentication Type	Represents the total number of VRRP packets received with unknown authentication type.
Authentication Type Mismatch	Represents the total number of VRRP advertisements received for which 'auth type' not equal to locally configured one for this virtual router.
Packet Length Errors	Represents the total number of VRRP packets received with packet length less than length of VRRP header.

show ip vrrp

This command displays whether VRRP functionality is enabled or disabled on the FASTPATH switch. It also displays some global parameters which are required for monitoring This command takes no options.

Format	**`show ip vrrp`**
Modes	Privileged EXEC User EXEC

TABLE 4-13 Entry Definitions for `show ip vrrp`

Entry	Definition
VRRP Admin Mode	Displays the administrative mode for VRRP functionality on the switch.
Router Checksum Errors	Represents the total number of VRRP packets received with an invalid VRRP checksum value.
Router Version Errors	Represents the total number of VRRP packets received with Unknown or unsupported version number.
Router VRID Errors	Represents the total number of VRRP packets received with invalid VRID for this virtual router.

show ip vrrp interface

This command displays all configuration information and VRRP router statistics of a virtual router configured on a specific interface.

Format	**`show ip vrrp interface`** *`<slot/port> <vrid>`*
Modes	Privileged EXEC User EXEC

TABLE 4-14 Entry Definitions for `show ip vrrp interface`

Entry	Definition
IP Address	This field represents the configured IP Address for the Virtual router.
VMAC address	Represents the VMAC address of the specified router.
Authentication type	Represents the authentication type for the specific virtual router.
Priority	Represents the priority value for the specific virtual router.
Advertisement interval	Represents the advertisement interval for the specific virtual router.
Pre-Empt Mode	Is the preemption mode configured on the specified virtual router.
Administrative Mode	Represents the status (Enable or Disable) of the specific router.
State	Represents the state (Master/backup) of the virtual router.

show ip vrrp interface brief

This command displays information about each virtual router configured on the FASTPATH switch. This command takes no options. It displays information about each virtual router.

Format	**`show ip vrrp interface brief`**
Modes	Privileged EXEC User EXEC

TABLE 4-15 Entry Definitions for `show ip vrrp interface brief`

Entry	Definition
Interface	Valid slot and port number separated by forward slashes.
VRID	Represents the router ID of the virtual router.
IP Address	The virtual router IP address.
Mode	Represents whether the virtual router is enabled or disabled.
State	Represents the state (Master/backup) of the virtual router.

VRRP Tracking Commands

This section describes the commands for tracking VRRP. The configuration of VRRP tracking is accomplished with two logical steps:

1. Configure the events that can impact VRRP priority change by defining tracking objects.
2. Link between VRRP priority changes and tracking objects by specifying VRRP priority change for state change in the tracked objects.

A `track` command object can track an interface property or IP layer properties. An interface might be tracked by its line-protocol state (up/down) or by its IP routing state (enable/disable). Use the commands in this section according to the preferred tracking method.

track interface line-protocol

This command tracks the link state of an interface. The object will be up when the interface is linked.

Default	none
Format	**track** <*object-number*> **interface** <*unit/port*> **line-protocol**
Modes	Global Config

track interface ip routing

This command tracks the state of a local ip route.

Default	none
Format	**track** <*object-number*> **interface** <*unit/port*> **ip routing**
Modes	Global Config

An IP-routing object is considered up when the following criteria exists:

- IP routing is enabled and active on the interface
- Interface line-protocol state is up

- Interface IP address is known (The IP address is configured or received through the Dynamic Host Configuration Protocol (DHCP) or IP Control Protocol (IPCP) negotiation.)

An IP-routing object is considered down when *one* of the following criteria exist:

- IP routing is disabled globally
- Interface line-protocol state is down
- Interface IP address is unknown (The IP address is not configured or received through DHCP or IPCP negotiation.)

track ip route reachability

This command tracks the state of a local ip route.

Default	none
Format	**track** *<object-number>* **ip route** *<ip-address/prefix-length>* **reachability**
Modes	Global Config

no track

This command removes the track with the given object number..

Format	**no track** *<object-number>*
Modes	Global Config

vrrp

This command assocates a track object with a VRRP instance. When the tracked object is down, the VRRP instance's priority will be decremented by *<decrement priority>*..

Format	**vrrp** *<vrID>* **`track`** *`<object-number>`* *`<decrement priority>`*
Modes	Global Config

`vrrp`

This command removes the specified track object from a specificed VRRP instance..

Format	**no vrrp** *<vrID>* **`track`** *`<object-number>`*
Modes	Global Config

`show track`

This command displays all configuration information for VRRP track objects.

Format	**`show track`** *`<object-number>`*
Modes	Privileged EXEC User EXEC

TABLE 4-16 Entry Definitions for `show track`

Entry	**Definition**
Interface	Represents the interface the track object is monitoring.
Track ID	Represents the tracked objects ID number.
Attribute	Represents this particular track object's type.

`show ip vrrp track`

This command displays the current status of all tracks associated with <vrID>.

Format	**`show ip vrrp track`** *`<vrID>`*
Modes	Privileged EXEC User EXEC

TABLE 4-17 Entry Definitions for `show ip vrrp track`

Entry	Definition
Priority Dec	Represents the amount the given track object is decrementing the priority of the VRRP instance.
Interface	Represents the interface the track object is monitoring.
Track ID	Represents the tracked objects ID number.
Attribute	Represents this particular track object's type.

DHCP and BOOTP Relay Commands

This section describes the commands you use 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

`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

bootpdhcprelay enable

This command enables the forwarding of relay requests for BootP/DHCP Relay on the system.

Default	disabled
Format	**`bootpdhcprelay enable`**
Mode	Global Config

no bootpdhcprelay enable

This command disables the forwarding of relay requests for BootP/DHCP Relay on the system.

Format	**`no bootpdhcprelay enable`**
Mode	Global 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

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

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

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

bootpdhcprelay serverip

This command configures the server IP Address for BootP/DHCP Relay on the system. The <*`ipaddr`*> parameter is an IP address in a 4-digit dotted decimal format.

Default	0.0.0.0
Format	**`bootpdhcprelay serverip`** *`<ipaddr>`*
Mode	Global Config

no bootpdhcprelay serverip

This command configures the default server IP Address for BootP/DHCP Relay on the system.

Format	**`no bootpdhcprelay serverip`**
Mode	Global Config

`show bootpdhcprelay`

This command displays the BootP/DHCP Relay information.

Format	**`show bootpdhcprelay`**
Modes	Privileged EXEC User EXEC

TABLE 4-18 Entry Definitions for `show bootpdhcprelay`

Entry	**Definition**
Maximum Hop Count	Is the maximum allowable relay agent hops.
Minimum Wait Time (Seconds)	Is the minimum wait time.
Admin Mode	Represents whether relaying of requests is enabled or disabled.
Server IP Address	Is the IP Address for the BootP/DHCP Relay server.
Circuit Id Option Mode	Is the DHCP circuit Id option which may be enabled or disabled.
Requests Received	Is the number or requests received.
Requests Relayed	Is the number of requests relayed.
Packets Discarded	Is the number of packets discarded.

Open Shortest Path First (OSPF) Commands

This section describes the commands you use to view and configure OSPF, which is a link-state routing protocol that you use to route traffic within a network.

router ospf

Use this command to enter Router OSPF mode.

Format	**`router ospf`**
Mode	Global Config

enable (OSPF)

This command resets the default administrative mode of OSPF in the router (active).

Default	enabled
Format	**`enable`**
Mode	Router OSPF Config

no enable (OSPF)

This command sets the administrative mode of OSPF in the router to inactive.

Format	**`no enable`**
Mode	Router OSPF Config

ip ospf

This command enables OSPF on a router interface.

Default	disabled
Format	**`ip ospf`**
Mode	Interface Config

no ip ospf

This command disables OSPF on a router interface.

Format	**`no ip ospf`**
Mode	Interface Config

1583compatibility

This command enables OSPF 1583 compatibility.

Note – 1583 compatibility mode is enabled by default. If all OSPF routers in the routing domain are capable of operating according to RFC 2328, OSPF 1583 compatibility mode should be disabled.

Default	enabled
Format	**`1583compatibility`**
Mode	Router OSPF Config

no 1583compatibility

This command disables OSPF 1583 compatibility.

Format	**`no 1583compatibility`**
Mode	Router OSPF Config

area default-cost (OSPF)

This command configures the default cost for the stub area. You must specify the area ID and an integer value between 1-16777215.

Format	**`area`** *`<areaid>`* **`default-cost`** *`<1-16777215>`*
Mode	Router OSPF Config

area nssa (OSPF)

This command configures the specified areaid to function as an NSSA.

Format	**`area`** *`<areaid>`* **`nssa`**
Mode	Router OSPF Config

no area nssa

This command disables nssa from the specified area id.

Format	**`no area`** *`<areaid>`* **`nssa`**
Mode	Router OSPF Config

area nssa default-info-originate (OSPF)

This command configures the metric value and type for the default route advertised into the NSSA. The optional metric parameter specifies the metric of the default route and is to be in a range of 1-16777214. If no metric is specified, the default value is ****. The metric type can be comparable (nssa-external 1) or non-comparable (nssa-external 2).

Format	**`area`** *`<areaid>`* **`nssa default-info-originate`** *`[<metric>] [{comparable	non-comparable}]`*
Mode	Router OSPF Config

area nssa no-redistribute (OSPF)

This command configures the NSSA Area Border router (ABR) so that learned external routes will not be redistributed to the NSSA.

Format	**`area`** *`<areaid>`* **`nssa no-redistribute`**
Mode	Router OSPF Config

area nssa no-summary (OSPF)

This command configures the NSSA so that summary LSAs are not advertised into the NSSA.

Format	**area** *<areaid>* **nssa no-summary**
Mode	Router OSPF Config

area nssa translator-role (OSPF)

This command configures the translator role of the NSSA. A value of *always* causes the router to assume the role of the translator the instant it becomes a border router and a value of *candidate* causes the router to participate in the translator election process when it attains border router status.

Format	**area** *<areaid>* **nssa translator-role** *{always | candidate}*
Mode	Router OSPF Config

area nssa translator-stab-intv (OSPF)

This command configures the translator *<stabilityinterval>* of the NSSA. The *<stabilityinterval>* is the period of time that an elected translator continues to perform its duties after it determines that its translator status has been deposed by another router.

Format	**area** *<areaid>* **nssa translator-stab-intv** *<stabilityinterval>*
Mode	Router OSPF Config

area range (OSPF)

This command creates a specified area range for a specified NSSA. The *<ipaddr>* is a valid IP address. The *<subnetmask>* is a valid subnet mask. The LSDB type must be specified by either **summarylink** or **nssaexternallink**, and the advertising of the area range can be allowed or suppressed.

Format	**area** *<areaid>* **range** *<ipaddr> <subnetmask> {summarylink | nssaexternallink} [advertise | not-advertise]*
Mode	Router OSPF Config

no area range

This command deletes a specified area range. The *<ipaddr>* is a valid IP address. The *<subnetmask>* is a valid subnet mask.

Format	**no area** *<areaid>* **range** *<ipaddr> <subnetmask>*
Mode	Router OSPF Config

area stub (OSPF)

This command creates a stub area for the specified area ID. A stub area is characterized by the fact that AS External LSAs are not propagated into the area. Removing AS External LSAs and Summary LSAs can significantly reduce the link state database of routers within the stub area.

Format	**area** *<areaid>* **stub**
Mode	Router OSPF Config

no area stub

This command deletes a stub area for the specified area ID.

Format	**no area** *<areaid>* **stub**
Mode	Router OSPF Config

area stub no-summary (OSPF)

This command configures the Summary LSA mode for the stub area identified by *<areaid>*. Use this command to prevent LSA Summaries from being sent.

Default	disabled
Format	`area <areaid> stub no-summary`
Mode	Router OSPF Config

no area stub no-summary

This command configures the default Summary LSA mode for the stub area identified by *<areaid>*.

Format	`no area <areaid> stub no-summary`
Mode	Router OSPF Config

area virtual-link (OSPF)

This command creates the OSPF virtual interface for the specified *<areaid>* and *<neighbor>*. The *<neighbor>* parameter is the Router ID of the neighbor.

Format	`area <areaid> virtual-link <neighbor>`
Mode	Router OSPF Config

no area virtual-link

This command deletes the OSPF virtual interface from the given interface, identified by *<areaid>* and *<neighbor>*. The *<neighbor>* parameter is the Router ID of the neighbor.

Format	`no area <areaid> virtual-link <neighbor>`
Mode	Router OSPF Config

area virtual-link authentication

This command configures the authentication type and key for the OSPF virtual interface identified by *<areaid>* and *<neighbor>*. The *<neighbor>* parameter is the Router ID of the neighbor. The value for *<type>* is either none, simple, or encrypt. The *[key]* is composed of standard displayable, non-control keystrokes from a Standard 101/102-key keyboard. The authentication key must be 8 bytes or less if the authentication type is simple. If the type is encrypt, the key may be up to 256 bytes. Unauthenticated interfaces do not need an authentication key. If the type is encrypt, a key id in the range of 0 and 255 must be specified.The default value for authentication type is none. Neither the default password key nor the default key id are configured.

Default	none
Format	**area** *<areaid>* **virtual-link** *<neighbor>* **authentication** *{none | {simple <key>} | {encrypt <key> <keyid>}}*
Mode	Router OSPF Config

no area virtual-link authentication

This command configures the default authentication type for the OSPF virtual interface identified by *<areaid>* and *<neighbor>*. The *<neighbor>* parameter is the Router ID of the neighbor.

Format	**no area** *<areaid>* **virtual-link** *<neighbor>* **authentication**
Mode	Router OSPF Config

area virtual-link dead-interval (OSPF)

This command configures the dead interval for the OSPF virtual interface on the virtual interface identified by *<areaid>* and *<neighbor>*. The *<neighbor>* parameter is the Router ID of the neighbor. The range for seconds is 1 to 65535.

Default	40
Format	**`area`** *`<areaid>`* **`virtual-link`** *`<neighbor>`* **`dead-interval`** *`<seconds>`*
Mode	Router OSPF Config

no area virtual-link dead-interval

This command configures the default dead interval for the OSPF virtual interface on the virtual interface identified by *<areaid>* and *<neighbor>*. The *<neighbor>* parameter is the Router ID of the neighbor.

Format	**`no area`** *`<areaid>`* **`virtual-link`** *`<neighbor>`* **`dead-interval`**
Mode	Router OSPF Config

area virtual-link hello-interval (OSPF)

This command configures the hello interval for the OSPF virtual interface on the virtual interface identified by *<areaid>* and *<neighbor>*. The *<neighbor>* parameter is the Router ID of the neighbor. The range for *<seconds>* is 1 to 65535.

Default	10
Format	**`area`** *`<areaid>`* **`virtual-link`** *`<neighbor>`* **`hello-interval`** *`<1-65535>`*
Mode	Router OSPF Config

no area virtual-link hello-interval

This command configures the default hello interval for the OSPF virtual interface on the virtual interface identified by <*areaid*> and <*neighbor*>. The <*neighbor*> parameter is the Router ID of the neighbor.

Format	**no area** <*areaid*> **virtual-link** <*neighbor*> **hello-interval**
Mode	Router OSPF Config

area virtual-link retransmit-interval (OSPF)

This command configures the retransmit interval for the OSPF virtual interface on the virtual interface identified by <*areaid*> and <*neighbor*>. The <*neighbor*> parameter is the Router ID of the neighbor. The range for seconds is 0 to 3600.

Default	5
Format	**area** <*areaid*> **virtual-link** <*neighbor*> **retransmit-interval** <*seconds*>
Mode	Router OSPF Config

no area virtual-link retransmit-interval

This command configures the default retransmit interval for the OSPF virtual interface on the virtual interface identified by <*areaid*> and <*neighbor*>. The <*neighbor*> parameter is the Router ID of the neighbor.

Format	**no area** <*areaid*> **virtual-link** <*neighbor*> **retransmit-interval**
Mode	Router OSPF Config

area virtual-link transmit-delay (OSPF)

This command configures the transmit delay for the OSPF virtual interface on the virtual interface identified by **<***areaid***>** and **<***neighbor***>**. The **<***neighbor***>** parameter is the Router ID of the neighbor. The range for seconds is 0 to 3600 (1 hour).

Default	1
Format	**area** <*areaid*> **virtual-link** <*neighbor*> **transmit-delay** <*seconds*>
Mode	Router OSPF Config

no area virtual-link transmit-delay

This command resets the default transmit delay for the OSPF virtual interface to the default value.

Format	**no area** <*areaid*> **virtual-link** <*neighbor*> **transmit-delay**
Mode	Router OSPF Config

default-information originate (OSPF)

This command is used to control the advertisement of default routes.

Default	metric—unspecified type—2
Format	**default-information originate** *[always] [metric <0-16777214>] [metric-type {1 | 2}]*
Mode	Router OSPF Config

no default-information originate (OSPF)

This command is used to control the advertisement of default routes.

Format	**`no default-information originate`** *`[metric] [metric-type]`*
Mode	Router OSPF Config

default-metric (OSPF)

This command is used to set a default for the metric of distributed routes.

Format	**`default-metric`** *`<1-16777214>`*
Mode	Router OSPF Config

no default-metric (OSPF)

This command is used to set a default for the metric of distributed routes.

Format	**`no default-metric`**
Mode	Router OSPF Config

distance ospf (OSPF)

This command sets the route preference value of OSPF in the router. Lower route preference values are preferred when determining the best route. The type of OSPF can be intra, inter, type-1, or type-2. The OSPF specification (RFC 2328) requires that preferences must be given to the routes learned via OSPF in the following order: intra < inter < type-1 < type-2. The *<preference>* range is 1 to 255. A route with a preference of 255 cannot be used to forward traffic.

Default	intra—8 inter—10 type-1—13 type-2—50.
Format	**`distance ospf`** *`{intra	inter	type1	type2} <preference>`*
Mode	Router OSPF Config

no distance ospf

This command sets the default route preference value of OSPF in the router. The type of OSPF can be intra, inter, type-1, or type-2.

Format	**`no distance ospf`** *`{intra	inter	type1	type2}`*
Mode	Router OSPF Config

distribute-list out (OSPF)

Use this command to specify the access list to filter routes received from the source protocol.

Format	**`distribute-list`** *`<1-199>`* **`out`** *`{rip	bgp	static	connected}`*
Mode	Router OSPF Config

no distribute-list out

Use this command to specify the access list to filter routes received from the source protocol.

Format	**`no distribute-list`** *`<1-199>`* **`out`** *`{rip	bgp	static	connected}`*
Mode	Router OSPF Config

exit-overflow-interval (OSPF)

This command configures the exit overflow interval for OSPF. It describes the number of seconds after entering Overflow state that a router will wait before attempting to leave the Overflow State. This allows the router to again originate non-default AS-external-LSAs. When set to 0, the router will not leave Overflow State until restarted. The range for seconds is 0 to 2147483647 seconds.

Default	0
Format	**`exit-overflow-interval`** *`<seconds>`*
Mode	Router OSPF Config

no exit-overflow-interval

This command configures the default exit overflow interval for OSPF.

Format	**`no exit-overflow-interval`**
Mode	Router OSPF Config

external-lsdb-limit (OSPF)

This command configures the external LSDB limit for OSPF. If the value is -1, then there is no limit. When the number of non-default AS-external-LSAs in a router's link-state database reaches the external LSDB limit, the router enters overflow state. The router never holds more than the external LSDB limit non-default AS-external-LSAs in it database. The external LSDB limit MUST be set identically in all routers attached to the OSPF backbone and/or any regular OSPF area. The range for limit is -1 to 2147483647.

Default	-1
Format	**`external-lsdb-limit`** *`<limit>`*
Mode	Router OSPF Config

no external-lsdb-limit

This command configures the default external LSDB limit for OSPF.

Format	**`no external-lsdb-limit`**
Mode	Router OSPF Config

ip ospf areaid

This command sets the OSPF area to which the specified router interface belongs. The *`<areaid>`* is an IP address, formatted as a 4-digit dotted-decimal number or a decimal value in the range of <0-4294967295>. The *`<areaid>`* uniquely identifies the area to which the interface connects. Assigning an area id, which does not exist on an interface, causes the area to be created with default values.

Format	**`ip ospf areaid <`***`areaid`*`>`
Mode	Interface Config

ip ospf authentication

This command sets the OSPF Authentication Type and Key for the specified interface. The value of <*`type`*> is either none, simple or encrypt. The [*`key`*] is composed of standard displayable, non-control keystrokes from a Standard 101/102-key keyboard. The authentication key must be 8 bytes or less if the authentication type is simple. If the type is encrypt, the key may be up to 256 bytes. If the 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 ospf authentication`** *`{none	{simple <key>}	{encrypt <key> <keyid>}}`*
Mode	Interface Config

no ip ospf authentication

This command sets the default OSPF Authentication Type for the specified interface.

Format	**`no ip ospf authentication`**
Mode	Interface Config

ip ospf cost

This command configures the cost on an OSPF interface. The <*cost*> parameter has a range of 1 to 65535.

Default	10
Format	**`ip ospf cost`** **<***1-65535***>**
Mode	Interface Config

no ip ospf cost

This command configures the default cost on an OSPF interface.

Format	**`no ip ospf cost`**
Mode	Interface Config

ip ospf dead-interval

This command sets the OSPF dead interval for the specified interface. The value for <*seconds*> is a valid positive integer, which represents the length of time in seconds that a router's Hello packets have not been seen before its neighbor routers declare that the router is down. The value for the length of time must be the same for all routers attached to a common network. This value should be some multiple of the Hello Interval (i.e. 4). Valid values range for seconds is from 1 to 2147483647.

Default	40
Format	**`ip ospf dead-interval`** <*seconds*>
Mode	Interface Config

no ip ospf dead-interval

This command sets the default OSPF dead interval for the specified interface.

Format	**`no ip ospf dead-interval`**
Mode	Interface Config

ip ospf hello-interval

This command sets the OSPF hello interval for the specified interface. The value for seconds is a valid positive integer, which represents the length of time in seconds. The value for the length of time must be the same for all routers attached to a network.

Valid values range from 1 to 65535.

Default	10
Format	**`ip ospf hello-interval`** *`<seconds>`*
Mode	Interface Config

no ip ospf hello-interval

This command sets the default OSPF hello interval for the specified interface.

Format	**`no ip ospf hello-interval`**
Mode	Interface Config

ip ospf priority

This command sets the OSPF priority for the specified router interface. The priority of the interface is a priority integer from 0 to 255. A value of 0 indicates that the router is not eligible to become the designated router on this network.

Default	1, which is the highest router priority.
Format	**`ip ospf priority`** *`<0-255>`*
Mode	Interface Config

no ip ospf priority

This command sets the default OSPF priority for the specified router interface.

Format	**`no ip ospf priority`**
Mode	Interface Config

ip ospf retransmit-interval

This command sets the OSPF retransmit Interval for the specified interface. The retransmit interval is specified in seconds. The value for <*seconds*> is the number of seconds between link-state advertisement retransmissions for adjacencies belonging to this router interface. This value is also used when retransmitting database description and link-state request packets. Valid values range from 0 to 3600 (1 hour).

Default	5
Format	**`ip ospf retransmit-interval`** *<0-3600>*
Mode	Interface Config

no ip ospf retransmit-interval

This command sets the default OSPF retransmit Interval for the specified interface.

Format	**`no ip ospf retransmit-interval`**
Mode	Interface Config

ip ospf transmit-delay

This command sets the OSPF Transit Delay for the specified interface. The transmit delay is specified in seconds. In addition, it sets the estimated number of seconds it takes to transmit a link state update packet over this interface. Valid values for *<seconds>* range from 1 to 3600 (1 hour).

Default	1
Format	**`ip ospf transmit-delay`** *`<1-3600>`*
Mode	Interface Config

no ip ospf transmit-delay

This command sets the default OSPF Transit Delay for the specified interface.

Format	**`no ip ospf transmit-delay`**
Mode	Interface Config

ip ospf mtu-ignore

This command disables OSPF maximum transmission unit (MTU) mismatch detection. OSPF Database Description packets specify the size of the largest IP packet that can be sent without fragmentation on the interface. When a router receives a Database Description packet, it examines the MTU advertised by the neighbor. By default, if the MTU is larger than the router can accept, the Database Description packet is rejected and the OSPF adjacency is not established.

Default	enabled
Format	**`ip ospf mtu-ignore`**
Mode	Interface Config

no ip ospf mtu-ignore

This command enables the OSPF MTU mismatch detection.

Format	**`no ip ospf mtu-ignore`**
Mode	Interface Config

router-id (OSPF)

This command sets a 4-digit dotted-decimal number uniquely identifying the router ospf id. The <*ipaddress*> is a configured value.

Format	**`router-id`** *<ipaddress>*
Mode	Router OSPF Config

redistribute (OSPF)

This command configures OSPF protocol to allow redistribution of routes from the specified source protocol/routers.

Default	metric—unspecified type—2 tag—0
Format	**`redistribute`** *{rip | bgp | static | connected} [metric <0-16777214>] [metric-type {1 | 2}] [tag <0-4294967295>] [subnets]*
Mode	Router OSPF Config

no redistribute

This command configures OSPF protocol to prohibit redistribution of routes from the specified source protocol/routers.

Format	**`no redistribute`** *{rip | bgp | static | connected} [metric] [metric-type] [tag] [subnets]*
Mode	Router OSPF Config

maximum-paths (OSPF)

This command sets the number of paths that OSPF can report for a given destination where *maxpaths* is platform dependent.

Default	4
Format	**`maximum-paths`** *`<maxpaths>`*
Mode	Router OSPF Config

no maximum-paths

This command resets the number of paths that OSPF can report for a given destination back to its default value.

Format	**`no maximum-paths`**
Mode	Router OSPF Config

timers spf

Use this command to configure the SPF delay time and hold time. The valid range for both parameters is 0-65535 seconds.

Default	delay-time—5 hold-time—10
Format	**`timers spf`** *`<delay-time> <hold-time>`*
Mode	Router OSPF Config

trapflags (OSPF)

This command enables OSPF traps.

Default	enabled
Format	**`trapflags`**
Mode	Router OSPF Config

`no trapflags`

This command disables OSPF traps.

Format	**`no trapflags`**
Mode	Router OSPF Config

`show ip ospf`

This command displays information relevant to the OSPF router.

Format	**`show ip ospf`**
Mode	Privileged EXEC

Note – Some of the information below displays only if you enable OSPF and configure certain features.

TABLE 4-19 Entry Definitions for `show ip ospf`

Entry	Definition
Router ID	A 32-bit integer in dotted decimal format identifying the router, about which information is displayed. This is a configured value.
OSPF Admin Mode	Shows whether the administrative mode of OSPF in the router is enabled or disabled. This is a configured value.
ASBR Mode	Reflects whether the ASBR mode is enabled or disabled. Enable implies that the router is an autonomous system border router. Router automatically becomes an ASBR when it is configured to redistribute routes learnt from other protocol. The possible values for the ASBR status is enabled (if the router is configured to re-distribute routes learnt by other protocols) or disabled (if the router is not configured for the same).
RFC 1583 Compatibility	Reflects whether 1583 compatibility is enabled or disabled. This is a configured value.
ABR Status	Shows whether the router is an OSPF Area Border Router.
Exit Overflow Interval	Shows the number of seconds that, after entering OverflowState, a router will attempt to leave OverflowState.
External LSA Count	Shows the number of external (LS type 5) link-state advertisements in the link-state database.

TABLE 4-19 Entry Definitions for `show ip ospf` *(Continued)*

Entry	Definition
External LSA Checksum	Shows the sum of the LS checksums of external link-state advertisements contained in the link-state database.
New LSAs Originated	Shows the number of new link-state advertisements that have been originated.
LSAs Received	Shows the number of link-state advertisements received determined to be new instantiations.
External LSDB Limit	Shows the maximum number of non-default AS-external-LSAs entries that can be stored in the link-state database.
Default Metric	Default value for redistributed routes.
Default Route Advertise	Indicates whether the default routes received from other source protocols are advertised or not
Always	Shows whether default routes are always advertised.
Metric	Shows the metric for the advertised default routes. If the metric is not configured, this field is blank.
Metric Type	Shows whether the routes are External Type 1 or External Type 2.
Maximum Paths	Shows the maximum number of paths that OSPF can report for a given destination.
Redistributing	This field is a heading and appears only if you configure the system to take routes learned from a non-OSPF source and advertise them to its peers.
Source	Shows source protocol/routes that are being redistributed. Possible values are static, connected, BGP, or RIP.
Metric	Shows the metric of the routes being redistributed.
Metric Type	Shows whether the routes are External Type 1 or External Type 2.
Tag	Shows the decimal value attached to each external route.
Subnets	For redistributing routes into OSPF, the scope of redistribution for the specified protocol.
Distribute-List	Shows the access list used to filter redistributed routes.

show ip ospf area

This command displays information about the area. The <*areaid*> identifies the OSPF area that is being displayed.

Format	**`show ip ospf area`** *<areaid>*
Modes	Privileged EXEC User EXEC

TABLE 4-20 Entry Definitions for `show ip ospf area`

Entry	Definition
AreaID	Is the area id of the requested OSPF area.
External Routing	Is a number representing the external routing capabilities for this area.
Spf Runs	Is the number of times that the intra-area route table has been calculated using this area's link-state database.
Area Border Router Count	The total number of area border routers reachable within this area.
Area LSA Count	Total number of link-state advertisements in this area's link-state database, excluding AS External LSA's.
Area LSA Checksum	A number representing the Area LSA Checksum for the specified AreaID excluding the external (LS type 5) link-state advertisements.
Import Summary LSAs	Shows whether to import summary LSAs.
OSPF Stub Metric Value	Shows the metric value of the stub area. This field displays only if the area is a configured as a stub area. The following OSPF NSSA specific information displays *only* if the area is configured as an NSSA.
Import Summary LSAs	Shows whether to import summary LSAs into the NSSA.
Redistribute into NSSA	Shows whether to redistribute information into the NSSA.
Default Information Originate	Shows whether to advertise a default route into the NSSA
Default Metric	Shows the metric value for the default route advertised into the NSSA.
Default Metric Type	Shows the metric type for the default route advertised into the NSSA.

TABLE 4-20 Entry Definitions for `show ip ospf area` *(Continued)*

Entry	Definition
Translator Role	Shows the NSSA translator role of the ABR, which is always or candidate.
Translator Stability Interval	Shows the amount of time that an elected translator continues to perform its duties after it determines that its translator status has been deposed by another router.
Translator State	Shows whether the ABR translator state is disabled, always, or elected.

`show ip ospf border-routers`

This command displays the internal OSPF routing table entries to an Area Border Router (ABR) and Autonomous System Boundary Router (ASBR).

Format	**`show ip ospf border-routers`**
Modes	User EXEC Privileged EXEC

TABLE 4-21 Entry Definitions for `show ip ospf border-routers`

Entry	Definition
Type	The type of the route to the destination, which is one of the following values: • intra - Intra-area route • inter - Inter-area route
Router ID	Router ID of the destination.
Cost	Cost of using this route.
Area ID	The area ID of the area from which this route is learned.
Router Type	The router type of the destination; it is either an ABR or ASBR or both.
Next Hop	Address of the next hop toward the destination.
Next Hop Intf	The outgoing router interface to use when forwarding traffic to the next hop.

`show ip ospf database`

This command displays information about the link state database when OSPF is enabled. If you do not enter any parameters, the command displays the LSA headers for all areas.

- Use the optional *<areaid>* parameter to display database information about a specific area.
- Use the optional parameters to specify the type of link state advertisements to display.
- Use *asbr-summary* to show the autonomous system boundary router (ASBR) summary LSAs. Use *external* to display the external LSAs.
- Use *network* to display the network LSAs.
- Use *nssa-external* to display NSSA external LSAs.
- Use *router* to display router LSAs.
- Use *summary* to show the LSA database summary information.
- Use *<lsid>* to specify the link state ID (LSID). The value of *<lsid>* can be an IP address or an integer in the range of 0-4294967295.
- Use *adv-router* to show the LSAs that are restricted by the advertising router.
- Use *self-originate* to display the LSAs in that are self originated.

Format	**`show ip ospf`** *`[<areaid>]`* **`database`** *`[{asbr-summary	external	network	nssa-external	router	summary}] [<lsid>] [{adv-router [<rtrid>]	self-originate}]`*
Modes	Privileged EXEC User EXEC

For each link-type and area, the following information is displayed only if OSPF is enabled.

TABLE 4-22 Entry Definitions for `show ip ospf database`

Entry	Definition
Link Id	Is a number that uniquely identifies an LSA that a router originates from all other self originated LSA's of the same LS type.
Adv Router	The Advertising Router. Is a 32 bit dotted decimal number representing the LSDB interface.
Age	Is a number representing the age of the link state advertisement in seconds.
Sequence	Is a number that represents which LSA is more recent.
Checksum	Is the total number LSA checksum.
Options	This is an integer. It indicates that the LSA receives special handling during routing calculations.
Rtr Opt	Router Options are valid for router links only.

show ip ospf database database-summary

Use this command to display the number of each type of LSA in the database for each area and for the router. The command also displays the total number of LSAs in the database.

Format	**`show ip ospf database database-summary`**
Modes	Privileged EXEC User EXEC

TABLE 4-23 Entry Definitions for `show ip ospf database database-summary`

Entry	Definition
Router	Total number of router LSAs in the OSPF link state database.
Network	Total number of network LSAs in the OSPF link state database.
Summary Net	Total number of summary network LSAs in the database.
Summary ASBR	Number of summary ASBR LSAs in the database.
Type-7 Ext	Total number of Type-7 external LSAs in the database.
Self-Originated Type-7	Total number of self originated AS external LSAs in the OSPFv3 link state database.
Opaque Link	Number of opaque link LSAs in the database.
Opaque Area	Number of opaque area LSAs in the database.
Subtotal	Number of entries for the identified area.
Total	Number of entries for all areas.

show ip ospf interface

This command displays the information for the IFO object or virtual interface tables.

Format	**`show ip ospf interface`** *`{<slot/port> | loopback <loopback-id>}`*
Modes	Privileged EXEC User EXEC

TABLE 4-24 Entry Definitions for `show ip ospf interface`

Entry	Definition
IP Address	Represents the IP address for the specified interface.
Subnet Mask	A mask of the network and host portion of the IP address for the OSPF interface.
OSPF Admin Mode	States whether OSPF is enabled or disabled on a router interface.
OSPF Area ID	Represents the OSPF Area Id for the specified interface.
Router Priority	A number representing the OSPF Priority for the specified interface.
Retransmit Interval	A number representing the OSPF Retransmit Interval for the specified interface.
Hello Interval	A number representing the OSPF Hello Interval for the specified interface.
Dead Interval	A number representing the OSPF Dead Interval for the specified interface.
LSA Ack Interval	A number representing the OSPF LSA Acknowledgement Interval for the specified interface.
Transit Delay Interval	A number representing the OSPF Transit Delay for the specified interface.
Authentication Type	The OSPF Authentication Type for the specified interface are: none, simple, and encrypt. The following information is displayed only if OSPF is enabled.
OSPF Interface Type	Broadcast LANs, such as Ethernet and IEEE 802.5, take the value *`broadcast`*. The OSPF Interface Type will be 'broadcast'.
State	The OSPF Interface States are: down, loopback, waiting, point-to-point, designated router, and backup designated router.
Designated Router	The router ID representing the designated router.
Backup Designated Router	The router ID representing the backup designated router.
Number of Link Events	The number of link events.
Metric Cost	The cost of the OSPF interface.

show ip ospf interface brief

This command displays brief information for the IFO object or virtual interface tables.

Format	**`show ip ospf interface brief`**
Modes	Privileged EXEC User EXEC

TABLE 4-25 Entry Definitions for `show ip ospf interface brief`

Entry	Definition
Interface	Valid slot and port number separated by forward slashes.
OSPF Admin Mode	States whether OSPF is enabled or disabled on a router interface.
OSPF Area ID	Represents the OSPF Area Id for the specified interface.
Router Priority	A number representing the OSPF Priority for the specified interface.
Hello Interval	A number representing the OSPF Hello Interval for the specified interface.
Dead Interval	A number representing the OSPF Dead Interval for the specified interface.
Retransmit Interval	A number representing the OSPF Retransmit Interval for the specified interface.
Retransmit Delay Interval	A number representing the OSPF Transit Delay for the specified interface.
LSA Ack Interval	A number representing the OSPF LSA Acknowledgement Interval for the specified interface.

show ip ospf interface stats

This command displays the statistics for a specific interface. The information below will only be displayed if OSPF is enabled.

Format	**`show ip ospf interface stats`** *`<slot/port>`*
Modes	Privileged EXEC User EXEC

TABLE 4-26 Entry Definitions for `show ip ospf interface stats`

Entry	Definition
OSPF Area ID	The area id of this OSPF interface.
Area Border Router Count	The total number of area border routers reachable within this area. This is initially zero, and is calculated in each SPF pass.
AS Border Router Count	The total number of Autonomous System border routers reachable within this area.
Area LSA Count	The total number of link-state advertisements in this area's link-state database, excluding AS External LSAs.
IP Address	The IP address associated with this OSPF interface.
OSPF Interface Events	The number of times the specified OSPF interface has changed its state, or an error has occurred.
Virtual Events	The number of state changes or errors that occurred on this virtual link.
Neighbor Events	The number of times this neighbor relationship has changed state, or an error has occurred.
External LSA Count	The number of external (LS type 5) link-state advertisements in the link-state database.

show ip ospf neighbor

This command displays information about OSPF neighbors. If you do not specify a neighbor IP address, the output displays summary information in a table. If you specify an interface or tunnel, only the information for that interface or tunnel displays. The *<ip-address>* is the IP address of the neighbor, and when you specify this, detailed information about the neighbor displays. The information below only displays if OSPF is enabled and the interface has a neighbor.

Format	**show ip ospf neighbor [***interface <slot/port>***] [<ip-address>]**
Modes	Privileged EXEC User EXEC

If you do not specify an IP address, a table with the following columns displays for all neighbors or the neighbor associated with the interface that you specify.

TABLE 4-27 Entry Definitions for `show ip ospf neighbor`

Entry	Definition
Router ID	Shows the 4-digit dotted-decimal number of the neighbor router.
Priority	Displays the OSPF priority for the specified interface. The priority of an interface is a priority integer from 0 to 255. A value of '0' indicates that the router is not eligible to become the designated router on this network.
IP Address	Shows the IP address of the neighbor.
Interface	Shows the interface of the local router in slot/port format.
State	Shows the state of the neighboring routers. Possible values are as follows: • Down- initial state of the neighbor conversation - no recent information has been received from the neighbor. • Attempt - no recent information has been received from the neighbor but a more concerted effort should be made to contact the neighbor. • Init - an Hello packet has recently been seen from the neighbor, but bidirectional communication has not yet been established. • 2 way - communication between the two routers is bidirectional. • Exchange start - the first step in creating an adjacency between the two neighboring routers, the goal is to decide which router is the master and to decide upon the initial DD sequence number. • Exchange - the router is describing its entire link state database by sending Database Description packets to the neighbor. • Loading - Link State Request packets are sent to the neighbor asking for the more recent LSAs that have been discovered (but not yet received) in the Exchange state. • Full - the neighboring routers are fully adjacent and they will now appear in router-LSAs and network-LSAs.
Dead Time	Shows the amount of time, in seconds, to wait before the router assumes the neighbor is unreachable. If you specify an IP address for the neighbor router, the following fields display:
Interface	Valid slot and port number separated by forward slashes.
Neighbor IP Address	Shows the IP address of the neighbor router.
Interface Index	Shows the interface ID of the neighbor router.
Area ID	Shows the area ID of the OSPF area associated with the interface.

TABLE 4-27 Entry Definitions for `show ip ospf neighbor` *(Continued)*

Entry	Definition
Options	An integer value that indicates the optional OSPF capabilities supported by the neighbor. The neighbor's optional OSPF capabilities are also listed in its Hello packets. This enables received Hello Packets to be rejected (i.e., neighbor relationships will not even start to form) if there is a mismatch in certain crucial OSPF capabilities.
Router Priority	Displays the OSPF priority for the specified interface. The priority of an interface is a priority integer from 0 to 255. A value of '0' indicates that the router is not eligible to become the designated router on this network.
Dead Timer Due	Shows the amount of time, in seconds, to wait before the router assumes the neighbor is unreachable.
State	Shows the state of the neighboring routers.
Events	The number of times this neighbor relationship has changed state, or an error has occurred.
Retransmission Queue Length	Is an integer representing the current length of the retransmission queue of the specified neighbor router Id of the specified interface.

`show ip ospf range`

This command displays information about the area ranges for the specified <*areaid*>. The <*areaid*> identifies the OSPF area whose ranges are being displayed.

Format	**`show ip ospf range <`***`areaid`***`>`**
Modes	Privileged EXEC User EXEC

TABLE 4-28 Entry Definitions for `show ip ospf range`

Entry	Definition
Area ID	The area id of the requested OSPF area.
IP Address	An IP Address which represents this area range.
Subnet Mask	A valid subnet mask for this area range.
Lsdb Type	The type of link advertisement associated with this area range.
Advertisement	The status of the advertisement. Advertisement has two possible settings: enabled or disabled.

`show ip ospf statistics`

This command displays information about recent Shortest Path First (SPF) calculations. The SPF is the OSPF routing table calculation. The output lists the number of times the SPF has run for each OSPF area. A table follows this information. For each of the 15 most recent SPF runs, the table lists how long ago the SPF ran, how long the SPF took, and the reasons why the SPF was scheduled.

Format	**`show ip ospf statistics`**
Modes	Privileged EXEC User EXEC

TABLE 4-29 Entry Definitions for `show ip ospf statistics`

Entry	Definition
Delta T	How long ago the SPF ran. The time is in the format hh:mm:ss, giving the hours, minutes, and seconds since the SPF run.
SPF Duration	How long the SPF took in milliseconds.
Reason	The reason the SPF was scheduled. Reason codes are as follows: • R - a router LSA has changed • N - a network LSA has changed • SN - a type 3 network summary LSA has changed • SA - a type 4 ASBR summary LSA has changed • X - a type 5 or type 7 external LSA has changed

`show ip ospf stub table`

This command displays the OSPF stub table. The information below will only be displayed if OSPF is initialized on the switch.

Format	**`show ip ospf stub table`**
Modes	Privileged EXEC User EXEC

TABLE 4-30 Entry Definitions for `show ip stub table`

Entry	Definition
Area ID	Is a 32-bit identifier for the created stub area.
Type of Service	Is the type of service associated with the stub metric. FASTPATH only supports Normal TOS.
Metric Val	The metric value is applied based on the TOS. It defaults to the least metric of the type of service among the interfaces to other areas. The OSPF cost for a route is a function of the metric value.
Import Summary LSA	Controls the import of summary LSAs into stub areas.

show ip ospf virtual-link

This command displays the OSPF Virtual Interface information for a specific area and neighbor. The <*areaid*> parameter identifies the area and the <*neighbor*> parameter identifies the neighbor's Router ID.

Format	**show ip ospf virtual-link <*areaid*> <*neighbor*>**
Modes	Privileged EXEC User EXEC

TABLE 4-31 Entry Definitions for `show ip ospf virtual-link`

Entry	Definition
Area ID	The area id of the requested OSPF area.
Neighbor Router ID	The input neighbor Router ID.
Hello Interval	The configured hello interval for the OSPF virtual interface.
Dead Interval	The configured dead interval for the OSPF virtual interface.
Iftransit Delay Interval	The configured transit delay for the OSPF virtual interface.
Retransmit Interval	The configured retransmit interval for the OSPF virtual interface.

TABLE 4-31 Entry Definitions for `show ip ospf virtual-link` *(Continued)*

Entry	Definition
Authentication Type	The configured authentication type of the OSPF virtual interface.
State	The OSPF Interface States are: down, loopback, waiting, point-to-point, designated router, and backup designated router. This is the state of the OSPF interface.
Neighbor State	The neighbor state.

`show ip ospf virtual-link brief`

This command displays the OSPF Virtual Interface information for all areas in the system.

Format	**`show ip ospf virtual-link brief`**
Modes	Privileged EXEC User EXEC

TABLE 4-32 Entry Definitions for `show ip ospf virtual-link brief`

Entry	Definition
Area Id	The area id of the requested OSPF area.
Neighbor	The neighbor interface of the OSPF virtual interface.
Hello Interval	The configured hello interval for the OSPF virtual interface.
Dead Interval	The configured dead interval for the OSPF virtual interface.
Retransmit Interval	The configured retransmit interval for the OSPF virtual interface.
Transit Delay	The configured transit delay for the OSPF virtual interface.

Routing Information Protocol (RIP) Commands

This section describes the commands you use to view and configure RIP, which is a distance-vector routing protocol that you use to route 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.

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. 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, non-control 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 the interface 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 the interface 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	OSPF as source protocol:
	`redistribute ospf` *`[metric <0-15>] [match [internal] [external 1] [external 2] [nssa-external 1] [nssa-external-2]]`*
	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

TABLE 4-33 Entry Definitions for `show ip rip`

Entry	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.
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	Sets a default for the metric of redistributed routes.This field displays the default metric 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 (i.e. ip rip).

Format	**`show ip rip interface brief`**
Modes	Privileged EXEC User EXEC

TABLE 4-34 Entry Definitions for `show ip rip interface brief`

Entry	Definition
Interface	Valid slot and port number separated by forward slashes.
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.

TABLE 4-34 Entry Definitions for `show ip rip interface brief` *(Continued)*

Entry	Definition
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	RIP administrative mode of router RIP operation; enable activates, disable de-activates it.
Link State	The mode of the interface (up or down).

`show ip rip interface`

This command displays information related to a particular RIP interface.

Format	**`show ip rip interface`** *<slot/port>*
Modes	Privileged EXEC User EXEC

TABLE 4-35 Entry Definitions for `show ip rip interface`

Entry	Definition
Interface	Valid slot and port number separated by forward slashes. 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.
Both RIP Admin Mode	RIP administrative mode of router RIP operation; enable activates, disable de-activates it. This is a configured value.
Link State	Indicates 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.
Default Metric	A number which represents the metric used for default routes in RIP updates originated on the specified interface. This is a configured value. The following information will be invalid if the link state is down.

TABLE 4-35 Entry Definitions for `show ip rip interface` *(Continued)*

Entry	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.

CHAPTER 5

IPv6 Commands

This chapter describes the IPv6 commands available in the FASTPATH® CLI.

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. 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.

This chapter contains the following sections:

Tunnel Interface Commands

The commands in this section describe how to create, delete, and manage tunnel interfaces.Several different types of tunnels provide functionality to facilitate the transition of IPv4 networks to IPv6 networks. These tunnels are divided into two classes: configured and automatic. The distinction is that configured tunnels are explicitly configured with a destination or endpoint of the tunnel. Automatic tunnels, in contrast, infer the endpoint of the tunnel from the destination address of packets routed into the tunnel. To assign an IP address to the tunnel interface, see "ip address" on page 170. To assign an IPv6 address to the tunnel interface, see "ipv6 address" on page 254.

interface tunnel

Use this command to enter the Interface Config mode for a tunnel interface. The *<tunnel-id>* range is 0 to 7.

Format	**`interface tunnel`** *`<tunnel-id>`*
Mode	Global Config

no interface tunnel

This command removes the tunnel interface and associated configuration parameters for the specified tunnel interface.

Format	**`no interface tunnel`** *`<tunnel-id>`*
Mode	Global Config

tunnel source

This command specifies the source transport address of the tunnel, either explicitly or by reference to an interface.

Format	**`tunnel source`** *`{<ipv4-address>	<ethernet> <slot/port>}`*
Mode	Interface Config

tunnel destination

This command specifies the destination transport address of the tunnel.

Format	**`tunnel destination`** *`{<ipv4-address>}`*
Mode	Interface Config

tunnel mode ipv6ip

This command specifies the mode of the tunnel.

Format	**`tunnel mode ipv6ip`**
Mode	Interface Config

show interface tunnel

This command displays the parameters related to tunnel such as tunnel mode, tunnel source address and tunnel destination address.

Format	**`show interface tunnel`** *`[<tunnel-id>]`*
Mode	Privileged EXEC

If you do not specify a tunnel ID, the command shows the following information for each configured tunnel.

TABLE 5-1 Entry Definitions for `show interface tunnel`

Entry	Definition
Tunnel ID	Shows the tunnel identification number.
Interface	Shows the name of the tunnel interface.
Tunnel Mode	Shows the tunnel mode.
Source Address	Shows the source transport address of the tunnel.
Destination Address	Shows the destination transport address of the tunnel. If you specify a tunnel ID, the command shows the following information for the tunnel:
Interface Link Status	Shows whether the link is up or down.
MTU Size	Shows the maximum transmission unit for packets on the interface.
IPv6 Address/ Length	If you enable IPv6 on the interface and assign an address, the IPv6 address and prefix display.

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 170. To assign an IPv6 address to the loopback interface, see "ipv6 address" on page 254.

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.

TABLE 5-2 Entry Definitions for `show interface loopback`

Entry	**Definition**
Loopback ID	Shows the loopback ID associated with the rest of the information in the row.
Interface	Shows the interface name.
IP Address	Shows the IPv4 address of the interface
Received Packets	Shows the number of packets received on this interface.
Sent Packets	Shows the number of packets transmitted from this interface.
IPv6 Address	Shows the IPv6 address of this interface If you specify a loopback ID, the following information appears:
Interface Link Status	Shows whether the link is up or down.
IP Address	Shows the IPv4 address of the interface.

TABLE 5-2 Entry Definitions for `show interface loopback` *(Continued)*

Entry	Definition
IPv6 is enabled (disabled)	Show whether IPv6 is enabled on the interface
IPv6 Address/Length is	Shows the IPv6 address of the interface.
MTU size	Shows the maximum transmission size for packets on this interface, in bytes.

IPv6 Routing Commands

This section describes the IPv6 commands you use to configure IPv6 on the system and on the interfaces. This section also describes IPv6 management commands and show commands.

`ipv6 forwarding`

This command enables IPv6 forwarding on the router

Default	enabled
Format	**`ipv6 forwarding`**
Mode	Global Config

`no ipv6 forwarding`

This command disables ipv6 forwarding on the router.

Format	**`no ipv6 forwarding`**
Mode	Global Config

ipv6 unicast-routing

Use this command to enable the forwarding of IPv6 unicast datagrams.

Default	disabled
Format	**`ipv6 unicast-routing`**
Mode	Global Config

no ipv6 unicast-routing

Use this command to disable the forwarding of IPv6 unicast datagrams.

Format	**`no ipv6 unicast-routing`**
Mode	Global Config

ipv6 enable

Use this command to enable IPv6 routing on an interface, including tunnel and loopback interfaces, that has not been configured with an explicit IPv6 address. When you use this command, the interface is automatically configured with a link-local address. You do not need to use this command if you configured an IPv6 global address on the interface.

Default	disabled
Format	**`ipv6 enable`**
Mode	Interface Config

no ipv6 enable

Use this command to disable IPv6 routing on an interface.

Format	**`no ipv6 enable`**
Mode	Interface Config

ipv6 address

Use this command to configure an IPv6 address on an interface, including tunnel and loopback interfaces, and to enable IPv6 processing on this interface. You can assign multiple globally reachable addresses to an interface by using this command. You do not need to assign a link-local address by using this command since one is automatically created. The *<prefix>* field consists of the bits of the address to be configured. The *<prefix_length>* designates how many of the high-order contiguous bits of the address make up the prefix.

You can express IPv6 addresses in eight blocks. Also of note is that instead of a period, a colon now separates each block. For simplification, leading zeros of each 16 bit block can be omitted. One sequence of 16 bit blocks containing only zeros can be replaced with a double colon "::", but not more than one at a time (otherwise it is no longer a unique representation).

- **Dropping zeros:** 3ffe:ffff:100:f101:0:0:0:1 becomes 3ffe:ffff:100:f101::1
- **Local host:** 0000:0000:0000:0000:0000:0000:0000:0001 becomes ::1
- **Any host:** 0000:0000:0000:0000:0000:0000:0000:0000 becomes ::

The hexadecimal letters in the IPv6 addresses are not case-sensitive. An example of an IPv6 prefix and prefix length is 3ffe:1::1234/64.

The optional [eui-64] field designates that IPv6 processing on the interfaces was enabled using an EUI-64 interface ID in the low order 64 bits of the address. If you use this option, the value of *<prefix_length>* must be 64 bits.

Format	**`ipv6 address`** *`<prefix>/<prefix_length> [eui64]`*
Mode	Interface Config

no ipv6 address

Use this command to remove all IPv6 addresses on an interface or specified IPv6 address. The *<prefix>* parameter consists of the bits of the address to be configured. The *<prefix_length>* designates how many of the high-order contiguous bits of the address comprise the prefix.The optional *[eui-64]* field designates that IPv6 processing on the interfaces was enabled using an EUI-64 interface ID in the low order 64 bits of the address.

If you do not supply any parameters, the command deletes all the IPv6 addresses on an interface.

Format	**`no ipv6 address`** [*`<prefix>/<prefix_length>] [eui64]`*]
Mode	Interface Config

ipv6 route

Use this command to configure an IPv6 static route. The *`<ipv6-prefix>`* is the IPv6 network that is the destination of the static route. The *`<prefix_length>`* is the length of the IPv6 prefix — a decimal value (usually 0-64) that shows 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 *`<prefix_length>`*. The *`<next-hop-address>`* is the IPv6 address of the next hop that can be used to reach the specified network. The *`<preference>`* parameter is a value the router uses to compare this route with routes from other route sources that have the same destination. The range for *`<preference>`* is 1 - 255, and the default value is 1. The *`interface <slot/port>`* identifies direct static routes from point-to-point and broadcast interfaces, and must be specified when using a link-local address as the next hop. A route with a preference of 255 cannot be used to forward traffic.

Default	disabled
Format	**`ipv6 route`** *`<ipv6-prefix>/<prefix_length> {<next-hop-address> [<preference>] | interface <slot/port> <next-hop-address> [<preference>]}`*
Mode	Global Config

no ipv6 route

Use this command to delete an IPv6 static route. Use the command without the optional parameters to delete all static routes to the specified destination. Use the *`<preference>`* parameter to revert preference of a route to default preference.

Default	disabled
Format	**`no ipv6 route`** *`<ipv6-prefix>/<prefix_length> [{<next-hop-address> | interface <slot/port> <next-hop-address> | <preference>}]`*
Mode	Global Config

ipv6 mtu

This command sets the maximum transmission unit (MTU) size, in bytes, of IPv6 packets on an interface. This command replaces the default or link MTU with a new MTU value.

Note – The default MTU value for a tunnel interface is 1480. You cannot change this value.

Default	0 or link speed (MTU value (1500))
Format	**`ipv6 mtu`** *`<1280-1500>`*
Mode	Interface Config

no ipv6 mtu

This command resets maximum transmission unit value to default value.

Format	**`no ipv6 mtu`**
Mode	Interface Config

ipv6 nd dad attempts

This command sets the number of duplicate address detection probes transmitted. Duplicate address detection verifies that an IPv6 address on an interface is unique.

Default	1
Format	**`ipv6 nd dad attempts`** *`<0 - 600>`*
Mode	Interface Config

no ipv6 nd dad attempts

This command resets to number of duplicate address detection value to default value.

Format	**`no ipv6 nd dad attempts`**
Mode	Interface config

ipv6 nd managed-config-flag

This command sets the “managed address configuration” flag in router advertisements. When the value is true, end nodes use DHCPv6. When the value is false, end nodes automatically configure addresses.

Default	false
Format	**`ipv6 nd managed-config-flag`**
Mode	Interface Config

no ipv6 nd managed-config-flag

This command resets the “managed address configuration” flag in router advertisements to the default value.

Format	**`no ipv6 nd managed-config-flag`**
Mode	Interface Config

ipv6 nd ns-interval

This command sets the interval between router advertisements for advertised neighbor solicitations, in milliseconds. An advertised value of 0 means the interval is unspecified.

Default	0
Format	**`ipv6 nd ns-interval`** *{<1000-3600000> | 0}*
Mode	Interface Config

no ipv6 nd ns-interval

This command resets the neighbor solicit retransmission interval of the specified interface to the default value.

Format	**`no ipv6 nd ns-interval`**
Mode	Interface Config

ipv6 nd other-config-flag

This command sets the “other stateful configuration” flag in router advertisements sent from the interface.

Default	false
Format	**`ipv6 nd other-config-flag`**
Mode	Interface Config

no ipv6 nd other-config-flag

This command resets the “other stateful configuration” flag back to its default value in router advertisements sent from the interface.

Format	**`no ipv6 nd other-config-flag`**
Mode	Interface Config

ipv6 nd ra-interval

This command sets the transmission interval between router advertisements.

Default	600
Format	**`ipv6 nd ra-interval-max`** *`<4- 1800>`*
Mode	Interface Config

no ipv6 nd ra-interval

This command sets router advertisement interval to the default.

Format	**`no ipv6 nd ra-interval-max`**
Mode	Interface Config

ipv6 nd ra-lifetime

This command sets the value, in seconds, that is placed in the Router Lifetime field of the router advertisements sent from the interface. The *<lifetime>* value must be zero, or it must be an integer between the value of the router advertisement transmission interval and 9000. A value of zero means this router is not to be used as the default router.

Default	1800
Format	**`ipv6 nd ra-lifetime`** *<lifetime>*
Mode	Interface Config

no ipv6 nd ra-lifetime

This command resets router lifetime to the default value.

Format	**`no ipv6 nd ra-lifetime`**
Mode	Interface config

ipv6 nd reachable-time

This command sets the router advertisement time to consider a neighbor reachable after neighbor discovery confirmation. Reachable time is specified in milliseconds. A value of zero means the time is unspecified by the router.

Default	0
Format	**`ipv6 nd reachable-time`** *<0-4294967295>*
Mode	Interface Config

no ipv6 nd reachable-time

This command means reachable time is unspecified for the router.

Format	**`no ipv6 nd reachable-time`**
Mode	Interface Config

ipv6 nd suppress-ra

This command suppresses router advertisement transmission on an interface.

Default	disabled
Format	**`ipv6 nd suppress-ra`**
Mode	Interface Config

no ipv6 nd suppress-ra

This command enables router transmission on an interface

Format	**`no ipv6 nd suppress-ra`**
Mode	Interface Config

ipv6 nd prefix

This command sets the IPv6 prefixes to include in the router advertisement. The first optional parameter is the valid lifetime of the router, in seconds. You can specify a value or indicate that the lifetime value is infinite. The second optional parameter is the preferred lifetime of the router.

Default	valid-lifetime—604800 preferred-lifetime—2592000 autoconfig—enabled on-link—enabled
Format	**`ipv6 nd prefix`** `<prefix/prefix_length> [{<0-4294967295> | infinite} {<0-4294967295> | infinite}] [no-autoconfig off-link]`
Mode	Interface Config

ping ipv6

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 *`<ipv6-address>`* 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.

Format	**`ping ipv6`** *`<ipv6-address> [size <datagram-size>]`*
Mode	Privileged EXEC User Exec

ping ipv6 interface

Use this command to determine whether another computer is on the network. To use the command, configure the switch for network (in-band) connection. The source and target devices must have the ping utility enabled and running on top of TCP/IP. The switch can be pinged from any IP workstation with which the switch is connected through the default VLAN (VLAN 1), as long as there is a physical path between the switch and the workstation. The terminal interface sends three pings to the target station. 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, tunnel, or logical interface as the source. Use the optional `size` keyword to specify the size of the ping packet. The *<ipv6-address>* is the IPv6 address of the device you want to query.

Format	**ping ipv6 interface** *{<slot/port> | tunnel <tunnel-id>} | loopback <loopback-id>} {link-local-address <link-local-address> | <ipv6-address>} [size <datagram-size>]*
Mode	Privileged EXEC User Exec

traceroute ipv6

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

Format	**traceroute ipv6** *<ipv6-address> [<port>]*
Mode	Privileged EXEC

show ipv6 brief

Use this command to display the IPv6 status of forwarding mode and IPv6 unicast routing mode.

Format	**show ipv6 brief**
Mode	Privileged EXEC

TABLE 5-3

Entry	Definition
IPv6 Forwarding Mode	Shows whether the IPv6 forwarding mode is enabled.
IPv6 Unicast Routing Mode	Shows whether the IPv6 unicast routing mode is enabled.

show ipv6 interface

Use this command to show the usability status of IPv6 interfaces.

Format	**`show ipv6 interface`** *`{brief	<slot/port>}`*
Mode	Privileged EXEC

If you use the brief parameter, the following information displays for all configured IPv6 interfaces.

TABLE 5-4 Entry Definitions for `show ipv6 interface`

Entry	Definition
Interface	Shows the interface in slot/port format.
IPv6 Routing Operational Mode	Shows whether the mode is enabled or disabled.
IPv6 Address/Length	Shows the IPv6 address and length on interfaces with IPv6 enabled. If you specify an interface, the following information also appears.
IPv6 is enabled	Appears if IPv6 is enabled on the interface.
Routing Mode	Shows whether IPv6 routing is enabled or disabled.
Administrative Mode	Shows whether the interface administrative mode is enabled or disabled.
Interface Maximum Transmission Unit	Shows the MTU size, in bytes.
Router Duplicate Address Detection Transmits	Shows the number of consecutive duplicate address detection probes to transmit.

TABLE 5-4 Entry Definitions for `show ipv6 interface` *(Continued)*

Entry	**Definition**
Router Advertisement NS Interval	Shows the interval, in milliseconds, between router advertisements for advertised neighbor solicitations.
Router Lifetime Interval	Shows the router lifetime value of the interface in router advertisements.
Router Advertisement Reachable Time	Shows the amount of time, in milliseconds, to consider a neighbor reachable after neighbor discovery confirmation.
Router Advertisement Interval	Shows the frequency, in seconds, that router advertisements are sent.
Router Advertisement Managed Config Flag	Shows whether the managed configuration flag is set (enabled) for router advertisements on this interface.
Router Advertisement Other Config Flag	Shows whether the other configuration flag is set (enabled) for router advertisements on this interface.
Router Advertisement Suppress Flag	Shows whether router advertisements are suppressed (enabled) or sent (disabled). If an IPv6 prefix is configured on the interface, the following information also appears.
IFPv6 Prefix is	Shows the IPv6 prefix for the specified interface.
Preferred Lifetime	Shows the amount of time the advertised prefix is a preferred prefix.
Valid Lifetime	Shows the amount of time the advertised prefix is valid.
Onlink Flag	Shows whether the onlink flag is set (enabled) in the prefix.
Autonomous Flag	Shows whether the autonomous address-configuration flag (autoconfig) is set (enabled) in the prefix.

show ipv6 neighbor

Use this command to display information about the IPv6 neighbors.

Format	**`show ipv6 neighbor`**
Mode	Privileged EXEC

TABLE 5-5 Entry Definitions for `show ipv6 neighbor`

Entry	Definition
Interface	Shows the interface in slot/port format.
IPv6 Address	IPV6 address of neighbor or interface
MAC Address	Link-layer Address
IsRtr	Shows whether the neighbor is a router. If the value is TRUE, the neighbor is known to be a router, and FALSE otherwise. A value of FALSE might not mean Note that routers are not always *known* to be routers.
Neighbor State	State of neighbor cache entry. Possible values are Incomplete, Reachable, Stale, Delay, Probe, and Unknown.
Last Updated	Shows the system uptime when the information for the neighbor was last updated.

clear ipv6 neighbors

Use this command to clear all entries IPv6 neighbor table or an entry on a specific interface. Use the *`<slot/port>`* parameter to specify the interface.

Format	**`clear ipv6 neighbors`** *`[<slot/port>]`*
Mode	Privileged EXEC

show ipv6 route

This command displays the IPv6 routing table.

- The *`<ipv6-address>`* specifies a specific IPv6 address for which the best-matching route would be displayed.
- The *`<ipv6-prefix/ipv6-prefix-length>`* specifies a specific IPv6 network for which the matching route would be displayed.

- The *<interface>* specifies that the routes with next-hops on the *<interface>* be displayed.
- The *<protocol>* specifies the protocol that installed the routes.
- The *<protocol>* is one of the following keywords: *connected*, *ospf*, *static*.
- The *all* specifies that all routes including best and non-best routes are displayed. Otherwise, only the best routes are displayed.

Note – If you use the *connected* keyword for *<protocol>*, the *all* option is not available because there are no best or non-best connected routes.

Format	**`show ipv6 route`** *`[{<ipv6-address> [<protocol>]	{{<ipv6-prefix/ipv6-prefix-length>	<unit/slot/port>} [<protocol>]	<protocol>	summary} [all]	all}]`*
Modes	Privileged EXEC User EXEC
Route Codes	Displays the key for the routing protocol codes that might appear in the routing table output.

The **`show ipv6 route`** command displays the routing tables in the following format:

```
Codes: C - connected, S - static
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF Ext 1, OE2 -
OSPF Ext 2
       ON1 - OSPF NSSA Ext Type 1, ON2 - OSPF NSSA Ext Type 2
```

The columns for the routing table display the following information.

TABLE 5-6 Entry Definitions for `show ipv6 route`

Entry	Definition
Code	The code for the routing protocol that created this routing entry.
IPv6-Prefix/ IPv6-Prefix-Length	The IPv6-Prefix and prefix-length of the destination IPv6 network corresponding to this route.
Preference/ Metric	The administrative distance (preference) and cost (metric) associated with this route. An example of this output is [1/0], where 1 is the preference and 0 is the metric.

TABLE 5-6 Entry Definitions for `show ipv6 route`

Entry	Definition
Tag	Displays the decimal value of the tag associated with a redistributed route, if it is not 0.
Next-Hop	The outgoing router IPv6 address to use when forwarding traffic to the next router (if any) in the path toward the destination
Interface	The outgoing router interface to use when forwarding traffic to the next destnation.

show ipv6 route preferences

Use this command to show the preference value associated with the type of route. Lower numbers have a greater preference. A route with a preference of 255 cannot be used to forward traffic.

Format	**`show ipv6 route preferences`**
Mode	Privileged EXEC

TABLE 5-7 Entry Definitions for `show ipv6 route preferences`

Entry	Definition
Local	Preference of directly-connected routes.
Static	Preference of static routes.
OSPF Intra	Preference of routes within the OSPF area.
OSPF Inter	Preference of routes to other OSPF routes that are outside of the area.
OSPF Ext T1	Preference of OSPF Type-1 external routes.
OSPF Ext T2	Preference of OSPF Type-2 external routes.
OSPF NSSA T1	Preference of OSPF NSSA Type 1 routes.
OSPF NSSA T2	Preference of OSPF NSSA Type 1 routes.

Note – The configuration of NSSA preferences is not supported in this release.

`show ipv6 route summary`

This command displays the summary of the routing table. Use *`all`* to display the count summary for all routes, including best and non-best routes. Use the command without parameters to display the count summary for only the best routes.

Format	**`show ipv6 route summary`** *`[all]`*
Modes	Privileged EXEC User EXEC

TABLE 5-8 Entry Definitions for `show ipv6 route summary`

Entry	Definition
Connected Routes	Total number of connected routes in the routing table.
Static Routes	Total number of static routes in the routing table.
OSPF Routes	Total number of routes installed by OSPFv3 protocol.
Number of Prefixes	Summarizes the number of routes with prefixes of different lengths
Total Routes	Shows the total number of routes in the routing table.

`show ipv6 vlan`

This command displays IPv6 VLAN routing interface addresses.

Format	**`show ipv6 vlan`**
Modes	Privileged EXEC User EXEC

TABLE 5-9 Entry Definitions for `show ipv6 vlan`

Entry	Definition
MAC Address used by Routing VLANs	Shows the MAC address.

TABLE 5-9 Entry Definitions for `show ipv6 vlan`

Entry	Definition
VLAN ID	Shows the VLAN ID of a configured VLAN.
Logical Interface	Shows the interface in slot/port format that is associated with the VLAN ID.
IPv6 Address/Prefix Length	Shows the IPv6 prefix and prefix length associated with the VLAN ID.

show ipv6 traffic

Use this command to show traffic and statistics for IPv6 and ICMPv6. Specify a logical, loopback, or tunnel interface to view information about traffic on a specific interface. If you do not specify an interface, the command displays information about traffic on all interfaces.

Format	**`show ipv6 traffic`** *`[{<slot/port> | loopback <loopback-id> | tunnel <tunnel-id>}]`*
Mode	Privileged EXEC

TABLE 5-10 Entry Definitions for `show ipv6 traffic`

Entry	Definition
Total Datagrams Received	Total number of input datagrams received by the interface, including those received in error.
Received Datagrams Locally Delivered	Total number of datagrams successfully delivered to IPv6 user-protocols (including ICMP). This counter increments at the interface to which these datagrams were addressed, which might not necessarily be the input interface for some of the datagrams.
Received Datagrams Discarded Due To Header Errors	Number of input datagrams discarded due to errors in their IPv6 headers, including version number mismatch, other format errors, hop count exceeded, errors discovered in processing their IPv6 options, etc.
Received Datagrams Discarded Due To MTU	Number of input datagrams that could not be forwarded because their size exceeded the link MTU of outgoing interface.
Received Datagrams Discarded Due To No Route	Number of input datagrams discarded because no route could be found to transmit them to their destination.

TABLE 5-10 Entry Definitions for `show ipv6 traffic` *(Continued)*

Entry	Definition
Received Datagrams With Unknown Protocol	Number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol. This counter increments at the interface to which these datagrams were addressed, which might not be necessarily the input interface for some of the datagrams.
Received Datagrams Discarded Due To Invalid Address	Number of input datagrams discarded because the IPv6 address in their IPv6 header's destination field was not a valid address to be received at this entity. This count includes invalid addresses (for example, ::0) and unsupported addresses (for example, addresses with unallocated prefixes). Forentities which are not IPv6 routers and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.
Received Datagrams Discarded Due To Truncated Data	Number of input datagrams discarded because datagram frame didn't carry enough data.
Received Datagrams Discarded Other	Number of input IPv6 datagrams for which no problems were encountered to prevent their continue processing, but which were discarded (e.g., for lack of buffer space). Note that this counter does not include datagrams discarded while awaiting re-assembly.
Received Datagrams Reassembly Required	Number of IPv6 fragments received which needed to be reassembled at this interface. Note that this counter increments at the interface to which these fragments were addressed, which might not be necessarily the input interface for some of the fragments.
Datagrams Successfully Reassembled	Number of IPv6 datagrams successfully reassembled. Note that this counter increments at the interface to which these datagrams were addressed, which might not be necessarily the input interface for some of the fragments.
Datagrams Failed To Reassemble	Number of failures detected by the IPv6 reassembly algorithm (for whatever reason: timed out, errors, etc.). Note that this is not necessarily a count of discarded IPv6 fragments since some algorithms (notably the algorithm in by combining them as they are received. This counter increments at the interface to which these fragments were addressed, which might not be necessarily the input interface for some of the fragments.
Datagrams Forwarded	Number of output datagrams which this entity received and forwarded to their final destinations. In entities which do not act as IPv6 routers, this counter will include only those packets which were Source-Routed via this entity, and the Source-Route processing was successful. Note that for a successfully forwarded datagram the counter of the outgoing interface increments.

TABLE 5-10 Entry Definitions for `show ipv6 traffic` *(Continued)*

Entry	Definition
Datagrams Locally Transmitted	Total number of IPv6 datagrams which local IPv6 user-protocols (including ICMP) supplied to IPv6 in requests for transmission. Note that this counter does not include any datagrams counted in ipv6IfStatsOutForwDatagrams.
Datagrams Transmit Failed	Number of output IPv6 datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (e.g., for lack of buffer space). Note that this counter would include datagrams counted in ipv6IfStatsOutForwDatagrams if any such packets met this (discretionary) discard criterion.
Fragments Created	Number of output datagram fragments that have been generated as a result of fragmentation at this output interface.
Datagrams Successfully Fragmented	Number of IPv6 datagrams that have been successfully fragmented at this output interface.
Datagrams Failed To Fragment	Number of IPv6 datagrams that have been discarded because they needed to be fragmented at this output interface but could not be.
Multicast Datagrams Received	Number of multicast packets received by the interface.
Multicast Datagrams Transmitted	Number of multicast packets transmitted by the interface.
Total ICMPv6 messages received	Total number of ICMP messages received by the interface which includes all those counted by ipv6IfIcmpInErrors. Note that this interface is the interface to which the ICMP messages were addressed which may not be necessarily the input interface for the messages.
ICMPv6 Messages with errors	Number of ICMP messages which the interface received but determined as having ICMP-specific errors (bad ICMP checksums, bad length, etc.).
ICMPv6 Destination Unreachable Messages	Number of ICMP Destination Unreachable messages received by the interface.
ICMPv6 Messages Prohibited Administratively	Number of ICMP destination unreachable/communication administratively prohibited messages received by the interface.
ICMPv6 Time Exceeded Messages	Number of ICMP Time Exceeded messages received by the interface.

TABLE 5-10 Entry Definitions for `show ipv6 traffic` *(Continued)*

Entry	Definition
ICMPv6 Parameter Problem Messages	Number of ICMP Parameter Problem messages received by the interface.
ICMPv6 messages with too big packets	Number of ICMP Packet Too Big messages received by the interface.
ICMPv6 Echo Request Messages Received	Number of ICMP Echo (request) messages received by the interface.
ICMPv6 Echo Reply Messages Received	Number of ICMP Echo Reply messages received by the interface.
ICMPv6 Router Solicit Messages Received	Number of ICMP Router Solicit messages received by the interface.
ICMPv6 Router Advertisement Messages Received	Number of ICMP Router Advertisement messages received by the interface.
ICMPv6 Neighbor Solicit Messages Received	Number of ICMP Neighbor Solicit messages received by the interface.
ICMPv6 Neighbor Advertisement Messages Received	Number of ICMP Neighbor Advertisement messages received by the interface.
ICMPv6 Redirect Messages Received	Number of Redirect messages received by the interface.
Transmitted	Number of ICMPv6 Group Membership Query messages received by the interface.
Total ICMPv6 Messages Transmitted	Total number of ICMP messages which this interface attempted to send. Note that this counter includes all those counted by icmpOutErrors.

TABLE 5-10 Entry Definitions for `show ipv6 traffic` *(Continued)*

Entry	Definition
ICMPv6 Messages Not Transmitted Due To Error	Number of ICMP messages which this interface did not send due to problems discovered within ICMP such as a lack of buffers. This value should not include errors discovered outside the ICMP layer such as the inability of IPv6 to route the resultant datagram. In some implementations there may be no types of error which contribute to this counter's value.
ICMPv6 Destination Unreachable Messages Transmitted	Number of ICMP Destination Unreachable messages sent by the interface.
ICMPv6 Messages Prohibited Administratively Transmitted	Number of ICMP destination unreachable/communication administratively prohibited messages sent.
ICMPv6 Time Exceeded Messages Transmitted	Number of ICMP Time Exceeded messages sent by the interface.
ICMPv6 Parameter Problem Messages Transmitted	Number of ICMP Parameter Problem messages sent by the interface.
ICMPv6 Packet Too Big Messages Transmitted	Number of ICMP Packet Too Big messages sent by the interface.
ICMPv6 Echo Request Messages Transmitted	Number of ICMP Echo (request) messages sent by the interface.ICMP echo messages sent
ICMPv6 Echo Reply Messages Transmitted	Number of ICMP Echo Reply messages sent by the interface.
ICMPv6 Router Solicit Messages Transmitted	Number of ICMP Router Solicitation messages sent by the interface.
ICMPv6 Router Advertisement Messages Transmitted	Number of ICMP Router Advertisement messages sent by the interface.

TABLE 5-10 Entry Definitions for `show ipv6 traffic` *(Continued)*

Entry	Definition
ICMPv6 Neighbor Solicit Messages Transmitted	Number of ICMP Neighbor Solicitation messages sent by the interface.
ICMPv6 Neighbor Advertisement Messages Transmitted	Number of ICMP Neighbor Advertisement messages sent by the interface.
ICMPv6 Redirect Messages Received	Number of Redirect messages sent. For a host, this object will always be zero, since hosts do not send redirects.
ICMPv6 Group Membership Query Messages Received	Number of ICMPv6 Group Membership Query messages sent.
ICMPv6 Group Membership Response Messages Received	Number of ICMPv6 group Membership Response messages sent.
ICMPv6 Group Membership Reduction Messages Received	Number of ICMPv6 Group Membership Reduction messages sent.
ICMPv6 Duplicate Address Detects	Number of duplicate addresses detected by the interface

clear ipv6 statistics

Use this command to clear IPv6 statistics for all interfaces or for a specific interface, including loopback and tunnel interfaces. IPv6 statistics display in the output of the **`show ipv6 traffic`** command. If you do not specify an interface, the counters for all IPv6 traffic statistics reset to zero.

Format	**`clear ipv6 statistics`** *`[{<slot/port>	loopback <loopback-id>	tunnel <tunnel-id>}]`*
Mode	Privileged EXEC

OSPFv3 Commands

This section describes the commands you use to configure OSPFv3, which is a link-state routing protocol that you use to route traffic within a network.

ipv6 ospf

This command enables OSPF on a router interface or loopback interface.

Default	disabled
Format	**`ipv6 ospf`**
Mode	Interface Config

no ipv6 ospf

This command disables OSPF on a router interface or loopback interface.

Format	**`no ipv6 ospf`**
Mode	Interface Config

ipv6 ospf areaid

This command sets the OSPF area to which the specified router interface belongs. The *`<areaid>`* is an IPv6 address, formatted as a 4-digit dotted-decimal number or a decimal value in the range of <0-4294967295>. The *`<areaid>`* uniquely identifies the area to which the interface connects. Assigning an area id, which does not exist on an interface, causes the area to be created with default values.

Format	**`ipv6 ospf areaid`** *`<areaid>`*
Mode	Interface Config

ipv6 ospf cost

This command configures the cost on an OSPF interface. The <*cost*> parameter has a range of 1 to 65535.

Default	10
Format	**`ipv6 ospf cost <`***`1-65535`***`>`**
Mode	Interface Config

no ipv6 ospf cost

This command configures the default cost on an OSPF interface.

Format	**`no ipv6 ospf cost`**
Mode	Interface Config

ipv6 ospf dead-interval

This command sets the OSPF dead interval for the specified interface. The value for <*seconds*> is a valid positive integer, which represents the length of time in seconds that a router's Hello packets have not been seen before its neighbor routers declare that the router is down. The value for the length of time must be the same for all routers attached to a common network. This value should be some multiple of the Hello Interval (i.e. 4). Valid values range for <*seconds*> is from 1 to 2147483647.

Default	40
Format	**`ipv6 ospf dead-interval`** *`<seconds>`*
Mode	Interface Config

no ipv6 ospf dead-interval

This command sets the default OSPF dead interval for the specified interface.

Format	**`no ipv6 ospf dead-interval`**
Mode	Interface Config

ipv6 ospf hello-interval

This command sets the OSPF hello interval for the specified interface. The value for <*seconds*> is a valid positive integer, which represents the length of time in seconds. The value for the length of time must be the same for all routers attached to a network.

Valid values for <*seconds*> range from 1 to 65535.

Default	10
Format	**`ipv6 ospf hello-interval`** *<seconds>*
Mode	Interface Config

no ipv6 ospf hello-interval

This command sets the default OSPF hello interval for the specified interface.

Format	**`no ipv6 ospf hello-interval`**
Mode	Interface Config

ipv6 ospf mtu-ignore

This command disables OSPF maximum transmission unit (MTU) mismatch detection. OSPF Database Description packets specify the size of the largest IP packet that can be sent without fragmentation on the interface. When a router receives a Database Description packet, it examines the MTU advertised by the neighbor. By default, if the MTU is larger than the router can accept, the Database Description packet is rejected and the OSPF adjacency is not established.

Default	enabled
Format	**`ipv6 ospf mtu-ignore`**
Mode	Interface Config

no ipv6 ospf mtu-ignore

This command enables the OSPF MTU mismatch detection.

Format	**`no ipv6 ospf mtu-ignore`**
Mode	Interface Config

ipv6 ospf network

This command changes the default OSPF network type for the interface. Normally, the network type is determined from the physical IP network type. By default all Ethernet networks are OSPF type broadcast. Similarly, tunnel interfaces default to point-to-point. When an Ethernet port is used as a single large bandwidth IP network between two routers, the network type can be point-to-point since there are only two routers. Using point-to-point as the network type eliminates the overhead of the OSPF designated router election. It is normally not useful to set a tunnel to OSPF network type broadcast.

Default	broadcast
Format	**`ipv6 ospf network`** *`{broadcast	point-to-point}`*
Mode	Interface Config

no ipv6 ospf network

This command sets the interface type to the default value.

Format	**`ipv6 ospf network`** *`{broadcast	point-to-point}`*
Mode	Interface Config

ipv6 ospf priority

This command sets the OSPF priority for the specified router interface. The priority of the interface is a priority integer from 0 to 255. A value of 0 indicates that the router is not eligible to become the designated router on this network.

Default	1, which is the highest router priority
Format	**`ipv6 ospf priority`** *`<0-255>`*
Mode	Interface Config

no ipv6 ospf priority

This command sets the default OSPF priority for the specified router interface.

Format	**`no ipv6 ospf priority`**
Mode	Interface Config

ipv6 ospf retransmit-interval

This command sets the OSPF retransmit Interval for the specified interface. The retransmit interval is specified in seconds. The value for <*`seconds`*> is the number of seconds between link-state advertisement retransmissions for adjacencies belonging to this router interface. This value is also used when retransmitting database description and link-state request packets. Valid values range from 0 to 3600 (1 hour).

Default	5
Format	**`ipv6 ospf retransmit-interval`** <*`seconds`*>
Mode	Interface Config

no ipv6 ospf retransmit-interval

This command sets the default OSPF retransmit Interval for the specified interface.

Format	**`no ipv6 ospf retransmit-interval`**
Mode	Interface Config

ipv6 ospf transmit-delay

This command sets the OSPF Transit Delay for the specified interface. The transmit delay is specified in seconds. In addition, it sets the estimated number of seconds it takes to transmit a link state update packet over this interface. Valid values for *<seconds>* range from 1 to 3600 (1 hour).

Default	1
Format	**`ipv6 ospf transmit-delay`** *<seconds>*
Mode	Interface Config

no ipv6 ospf transmit-delay

This command sets the default OSPF Transit Delay for the specified interface.

Format	**`no ipv6 ospf transmit-delay`**
Mode	Interface Config

ipv6 router ospf

Use this command to enter Router OSPFv3 Config mode.

Format	**`router ospf`**
Mode	Global Config

area default-cost (OSPFv3)

This command configures the monetary default cost for the stub area. The operator must specify the area id and an integer value between 1-16777215.

Format	**`area`** *`<areaid>`* **`default-cost`** *`<1-16777215>`*
Mode	Router OSPFv3 Config

area nssa (OSPFv3)

This command configures the specified areaid to function as an NSSA.

Format	**`area`** *`<areaid>`* **`nssa`**
Mode	Router OSPFv3 Config

no area nssa

This command disables nssa from the specified area id.

Format	**`no area`** *`<areaid>`* **`nssa`**
Mode	Router OSPFv3 Config

area nssa default-info-originate (OSPFv3)

This command configures the metric value and type for the default route advertised into the NSSA. The optional metric parameter specifies the metric of the default route and is to be in a range of 1-16777214. If no metric is specified, the default value is 10. The metric type can be comparable (nssa-external 1) or non-comparable (nssa-external 2).

Format	**`area`** *`<areaid>`* **`nssa default-info-originate`** *`[<metric>] [{comparable | non-comparable}]`*
Mode	Router OSPFv3 Config

area nssa no-redistribute (OSPFv3)

This command configures the NSSA ABR so that learned external routes will not be redistributed to the NSSA.

Format	**area** *<areaid>* **nssa no-redistribute**
Mode	Router OSPFv3 Config

area nssa no-summary (OSPFv3)

This command configures the NSSA so that summary LSAs are not advertised into the NSSA.

Format	**area** *<areaid>* **nssa no-summary**
Mode	Router OSPFv3 Config

area nssa translator-role (OSPFv3)

This command configures the translator role of the NSSA. A value of `always` causes the router to assume the role of the translator the instant it becomes a border router and a value of `candidate` causes the router to participate in the translator election process when it attains border router status.

Format	**area** *<areaid>* **nssa translator-role** *{always | candidate}*
Mode	Router OSPFv3 Config

area nssa translator-stab-intv (OSPFv3)

This command configures the translator *<stabilityinterval>* of the NSSA. The *<stabilityinterval>* is the period of time that an elected translator continues to perform its duties after it determines that its translator status has been deposed by another router.

Format	**area** *<areaid>* **nssa translator-stab-intv** *<stabilityinterval>*
Mode	Router OSPFv3 Config

area range (OSPFv3)

This command creates a specified area range for a specified NSSA. The *<ipaddr>* is a valid IP address. The *<subnetmask>* is a valid subnet mask. The LSDB type must be specified by either **summarylink** or **nssaexternallink**, and the advertising of the area range can be allowed or suppressed.

Format	**area** *<areaid>* **range** *<ipv6-prefix> <prefix-length> {summarylink | nssaexternallink} [advertise | not-advertise]*
Mode	Router OSPFv3 Config

no area range

This command deletes a specified area range. The *<ipaddr>* is a valid IP address. The *<subnetmask>* is a valid subnet mask.

Format	**no area** *<areaid>* **range** *<ipv6-prefix> <prefix-length>*
Mode	Router OSPFv3 Config

area stub (OSPFv3)

This command creates a stub area for the specified area ID. A stub area is characterized by the fact that AS External LSAs are not propagated into the area. Removing AS External LSAs and Summary LSAs can significantly reduce the link state database of routers within the stub area.

Format	**`area`** *`<areaid>`* **`stub`**
Mode	Router OSPFv3 Config

no area stub

This command deletes a stub area for the specified area ID.

Format	**`no area`** *`<areaid>`* **`stub`**
Mode	Router OSPFv3 Config

area stub no-summary (OSPFv3)

This command disables the import of Summary LSAs for the stub area identified by *`<areaid>`*.

Default	enabled
Format	**`area`** *`<areaid>`* **`stub no-summary`**
Mode	Router OSPFv3 Config

no area stub no-summary

This command sets the Summary LSA import mode to the default for the stub area identified by *`<areaid>`*.

Format	**`no area`** *`<areaid>`* **`stub summarylsa`**
Mode	Router OSPFv3 Config

area virtual-link (OSPFv3)

This command creates the OSPF virtual interface for the specified *<areaid>* and *<neighbor>*. The *<neighbor>* parameter is the Router ID of the neighbor.

Format	**area** *<areaid>* **virtual-link** *<neighbor>*
Mode	Router OSPFv3 Config

no area virtual-link

This command deletes the OSPF virtual interface from the given interface, identified by *<areaid>* and *<neighbor>*. The *<neighbor>* parameter is the Router ID of the neighbor.

Format	**no area** *<areaid>* **virtual-link** *<neighbor>*
Mode	Router OSPFv3 Config

area virtual-link dead-interval (OSPFv3)

This command configures the dead interval for the OSPF virtual interface on the virtual interface identified by *<areaid>* and *<neighbor>*. The *<neighbor>* parameter is the Router ID of the neighbor. The range for *<seconds>* is 1 to 65535.

Default	40
Format	**area** *<areaid>* **virtual-link** *<neighbor>* **dead-interval** *<seconds>*
Mode	Router OSPFv3 Config

no area virtual-link dead-interval

This command configures the default dead interval for the OSPF virtual interface on the virtual interface identified by <*areaid*> and <*neighbor*>. The <*neighbor*> parameter is the Router ID of the neighbor.

Format	**no area** <*areaid*> **virtual-link** <*neighbor*> **dead-interval**
Mode	Router OSPFv3 Config

area virtual-link hello-interval (OSPFv3)

This command configures the hello interval for the OSPF virtual interface on the virtual interface identified by <*areaid*> and <*neighbor*>. The <*neighbor*> parameter is the Router ID of the neighbor. The range for <*seconds*> is 1 to 65535.

Default	10
Format	**area** <*areaid*> **virtual-link** <*neighbor*> **hello-interval** <*seconds*>
Mode	Router OSPFv3 Config

no area virtual-link hello-interval

This command configures the default hello interval for the OSPF virtual interface on the virtual interface identified by <*areaid*> and <*neighbor*>. The <*neighbor*> parameter is the Router ID of the neighbor.

Format	**no area** <*areaid*> **virtual-link** <*neighbor*> **hello-interval**
Mode	Router OSPFv3 Config

area virtual-link retransmit-interval (OSPFv3)

This command configures the retransmit interval for the OSPF virtual interface on the virtual interface identified by *<areaid>* and *<neighbor>*. The *<neighbor>* parameter is the Router ID of the neighbor. The range for *<seconds>* is 0 to 3600.

Default	5
Format	**area** <*areaid*> **virtual-link** <*neighbor*> **retransmit-interval** <*seconds*>
Mode	Router OSPFv3 Config

no area virtual-link retransmit-interval

This command configures the default retransmit interval for the OSPF virtual interface on the virtual interface identified by <*areaid*> and <*neighbor*>. The <*neighbor*> parameter is the Router ID of the neighbor.

Format	**no area** <*areaid*> **virtual-link** <*neighbor*> **retransmit-interval**
Mode	Router OSPFv3 Config

area virtual-link transmit-delay (OSPFv3)

This command configures the transmit delay for the OSPF virtual interface on the virtual interface identified by <*areaid*> and <*neighbor*>. The <*neighbor*> parameter is the Router ID of the neighbor. The range for <*seconds*> is 0 to 3600 (1 hour).

Default	1
Format	**area** <*areaid*> **virtual-link** <*neighbor*> **transmit-delay** <*seconds*>
Mode	Router OSPFv3 Config

no area virtual-link transmit-delay

This command configures the default transmit delay for the OSPF virtual interface on the virtual interface identified by <*areaid*> and <*neighbor*>. The <*neighbor*> parameter is the Router ID of the neighbor.

Format	**no area** <*areaid*> **virtual-link** <*neighbor*> **transmit-delay**
Mode	Router OSPFv3 Config

default-information originate (OSPFv3)

This command is used to control the advertisement of default routes.

Default	metric—unspecified type—2
Format	**default-information originate** *[always] [metric <0-16777214>] [metric-type {1 | 2}]*
Mode	Router OSPFv3 Config

no default-information originate (OSPFv3)

This command is used to control the advertisement of default routes.

Format	**no default-information originate** *[metric] [metric-type]*
Mode	Router OSPFv3 Config

default-metric (OSPFv3)

This command is used to set a default for the metric of distributed routes.

Format	**default-metric** *<1-16777214>*
Mode	Router OSPFv3 Config

no default-metric (OSPFv3)

This command is used to set a default for the metric of distributed routes.

Format	**`no default-metric`**
Mode	Router OSPFv3 Config

distance ospf (OSPFv3)

This command sets the route preference value of OSPF in the router. Lower route preference values are preferred when determining the best route. The type of OSPF route can be intra, inter, type-1, or type-2. The OSPF specification (RFC 2328) requires that preferences must be given to the routes learned via OSPF in the following order: intra < inter < type-1 < type-2. The <*preference*> range is 1 to 255. A route with a preference of 255 cannot be used to forward traffic.

Default	intra—8 inter—10 type-1—13 type-2—50
Format	**`distance ospf`** *{intra | inter | type1 | type2} <preference>*
Mode	Router OSPFv3 Config

no distance ospf

This command sets the default route preference value of OSPF in the router. The type of OSPF route can be intra, inter, type-1, or type-2.

Format	**`no distance ospf`** *{intra | inter | type1 | type2}*
Mode	Router OSPFv3 Config

enable (OSPFv3)

This command resets the default administrative mode of OSPF in the router (active).

Default	enabled
Format	**`enable`**
Mode	Router OSPFv3 Config

no enable (OSPFv3)

This command sets the administrative mode of OSPF in the router to inactive.

Format	**`no enable`**
Mode	Router OSPFv3 Config

exit-overflow-interval (OSPFv3)

This command configures the exit overflow interval for OSPF. It describes the number of seconds after entering Overflow state that a router will wait before attempting to leave the Overflow State. This allows the router to again originate non-default AS-external-LSAs. When set to 0, the router will not leave Overflow State until restarted. The range for *<seconds>* is 0 to 2147483647 seconds.

Default	0
Format	**`exit-overflow-interval`** *<seconds>*
Mode	Router OSPFv3 Config

no exit-overflow-interval

This command configures the default exit overflow interval for OSPF.

Format	**`no exit-overflow-interval`**
Mode	Router OSPFv3 Config

external-lsdb-limit (OSPFv3)

This command configures the external LSDB limit for OSPF. If the value is -1, then there is no limit. When the number of non-default AS-external-LSAs in a router's link-state database reaches the external LSDB limit, the router enters overflow state. The router never holds more than the external LSDB limit non-default AS-external-LSAs in it database. The external LSDB limit MUST be set identically in all routers attached to the OSPF backbone and/or any regular OSPF area. The range for <`limit`> is -1 to 2147483647.

Default	-1
Format	**`external-lsdb-limit`** *<limit>*
Mode	Router OSPFv3 Config

no external-lsdb-limit

This command configures the default external LSDB limit for OSPF.

Format	**`no external-lsdb-limit`**
Mode	Router OSPFv3 Config

maximum-paths (OSPFv3)

This command sets the number of paths that OSPF can report for a given destination where *maxpaths* is platform dependent.

Default	4
Format	**`maximum-paths`** *<maxpaths>*
Mode	Router OSPFv3 Config

no maximum-paths

This command resets the number of paths that OSPF can report for a given destination back to its default value.

Format	**`no maximum-paths`**
Mode	Router OSPFv3 Config

redistribute (OSPFv3)

This command configures the OSPFv3 protocol to allow redistribution of routes from the specified source protocol/routers.

Default	metric—unspecified type—2 tag—0
Format	**`redistribute`** *`{static	connected} [metric <0-16777214>] [metric-type {1	2}] [tag <0-4294967295>]`*
Mode	Router OSPFv3 Config

no redistribute

This command configures OSPF protocol to prohibit redistribution of routes from the specified source protocol/routers.

Format	**`no redistribute`** *`{static	connected} [metric] [metric-type] [tag]`*
Mode	Router OSPFv3 Config

router-id (OSPFv3)

This command sets a 4-digit dotted-decimal number uniquely identifying the router ospf id. The <*ipaddress*> is a configured value.

Format	**`router-id`** *<ipaddress>*
Mode	Router OSPFv3 Config

trapflags

This command enables OSPF traps.

Default	enabled
Format	**`trapflags`**
Mode	Router OSPFv3 Config

no trapflags

This command disables OSPF traps.

Format	**`no trapflags`**
Mode	Router OSPFv3 Config

show ipv6 ospf

This command displays information relevant to the OSPF router.

Format	**`show ipv6 ospf`**
Mode	Privileged EXEC

Note – Some of the information below displays only if you enable OSPF and configure certain features.

TABLE 5-11 Entry Definitions for `show ipv6 ospf`

Entry	Definition
Router ID	Is a 32 bit integer in dotted decimal format identifying the router, about which information is displayed. This is a configured value.
OSPF Admin Mode	Shows whether the administrative mode of OSPF in the router is enabled or disabled. This is a configured value.
ASBR Mode	Reflects whether the ASBR mode is enabled or disabled. Enable implies that the router is an autonomous system border router. Router automatically becomes an ASBR when it is configured to redistribute routes learned from other protocol. The possible values for the ASBR status is enabled (if the router is configured to re-distribute routes learnt by other protocols) or disabled (if the router is not configured for the same).
ABR Status	Shows whether the router is an OSPF Area Border Router.
Exit Overflow Interval	Shows the number of seconds that, after entering Overflow State, a router will attempt to leave Overflow State.
External LSA Count	Shows the number of external (LS type 5) link-state advertisements in the link-state database.
External LSA Checksum	Shows the sum of the LS checksums of external link-state advertisements contained in the link-state database.
New LSAs Originated	Shows the number of new link-state advertisements that have been originated.
LSAs Received	Shows the number of link-state advertisements received determined to be new instantiations.
External LSDB Limit	Shows the maximum number of non-default AS-external-LSAs entries that can be stored in the link-state database.
Default Metric	Default value for redistributed routes.
Default Route Advertise	Indicates whether the default routes received from other source protocols are advertised or not
Always	Shows whether default routes are always advertised.
Metric	Shows the metric for the advertised default routes. If the metric is not configured, this field is blank.
Metric Type	Shows whether the routes are External Type 1 or External Type 2.
Maximum Paths	Shows the maximum number of paths that OSPF can report for a given destination.

TABLE 5-11 Entry Definitions for `show ipv6 ospf` *(Continued)*

Entry	Definition
Redistributing	This field is a heading and appears only if you configure the system to take routes learned from a non-OSPF source and advertise them to its peers.
Source	Shows source protocol/routes that are being redistributed. Possible values are static, connected, BGP, or RIP.
Metric	Shows the metric of the routes being redistributed.
Metric Type	Shows whether the routes are External Type 1 or External Type 2.
Tag	Shows the decimal value attached to each external route.
Subnets	For redistributing routes into OSPF, the scope of redistribution for the specified protocol.
Distribute-List	Shows the access list used to filter redistributed routes.

show ipv6 ospf area

This command displays information about the area. The <*areaid*> identifies the OSPF area that is being displayed.

Format	**show ipv6 ospf area** <*areaid*>
Modes	Privileged EXEC User EXEC

TABLE 5-12 Entry Definitions for `show ospf area`

Entry	Definition
AreaID	Is the area id of the requested OSPF area.
External Routing	Is a number representing the external routing capabilities for this area.
Spf Runs	Is the number of times that the intra-area route table has been calculated using this area's link-state database.
Area Border Router Count	The total number of area border routers reachable within this area.
Area LSA Count	Total number of link-state advertisements in this area's link-state database, excluding AS External LSAs.
Area LSA Checksum	A number representing the Area LSA Checksum for the specified AreaID excluding the external (LS type 5) link-state advertisements.
Stub Mode	Represents whether the specified Area is a stub area or not. The possible values are enabled and disabled. This is a configured value.

TABLE 5-12 Entry Definitions for `show ospf area` *(Continued)*

Entry	**Definition**
Import Summary LSAs	Shows whether to import summary LSAs (enabled).
OSPF Stub Metric Value	Shows the metric value of the stub area. This field displays only if the area is a configured as a stub area. The following OSPF NSSA specific information displays only if the area is configured as an NSSA.
Import Summary LSAs	Shows whether to import summary LSAs into the NSSA.
Redistribute into NSSA	Shows whether to redistribute information into the NSSA.
Default Information Originate	Shows whether to advertise a default route into the NSSA
Default Metric	Shows the metric value for the default route advertised into the NSSA.
Default Metric Type	Shows the metric type for the default route advertised into the NSSA.
Translator Role	Shows the NSSA translator role of the ABR, which is always or candidate.
Translator Stability Interval	Shows the amount of time that an elected translator continues to perform its duties after it determines that its translator status has been deposed by another router.
Translator State	Shows whether the ABR translator state is disabled, always, or elected.

`show ipv6 ospf border-routers`

This command displays ospfv3 routes to reach area border and AS border routers.

Format	**`show ipv6 ospf border-routers`**
Mode	Privileged EXEC

TABLE 5-13 Entry Definitions for `show ipv6 ospf border-routers`

Entry	Definition
Type	The type of the route to the destination, which is one of the following values: intra - Intra-area route inter - Inter-area route
Router ID	Router ID of the destination.
Cost	Cost of using this route.
Area ID	The area ID of the area from which this route is learned.
Router Type	The router type of the destination; it is either an ABR or ASBR or both.
Next Hop	Address of the next hop toward the destination.
Next Hop Intf	The outgoing router interface to use when forwarding traffic to the next hop.

show ipv6 ospf database

This command displays information about the link state database when OSPFv3 is enabled. If you do not enter any parameters, the command displays the LSA headers for all areas. Use the optional *<areaid>* parameter to display database information about a specific area. Use the other optional parameters to specify the type of link state advertisements to display. Use *external* to display the external LSAs. Use *inter-area* to display the inter-area LSAs. Use *link* to display the link LSAs. Use *network* to display the network LSAs. Use nssa-external to display NSSA external LSAs. Use *prefix* to display intra-area Prefix LSAs. Use *router* to display router LSAs. Use *unknown area*, *unknown as*, or *unknown link* to display unknown area, AS or link-scope LSAs, respectively. Use *<lsid>* to specify the link state ID (LSID). Use *adv-router* to show the LSAs that are restricted by the advertising router. Use *self-originate* to display the LSAs in that are self originated. The information below is only displayed if OSPF is enabled.

Format	**show ipv6 ospf** *[<areaid>]* **database** *[{external | inter-area {prefix | router} | link | network | nssa-external | prefix | router | unknown {area | as | link}}] [<lsid>] [{adv-router [<rtrid>] | self-originate}]*
Modes	Privileged EXEC User EXEC

For each link-type and area, the following information is displayed.

TABLE 5-14 Entry Definitions for `show ipv6 ospf database`

Entry	Definition
Link Id	Is a number that uniquely identifies an LSA that a router originates from all other self originated LSAs of the same LS type.
Adv Router	The Advertising Router. Is a 32 bit dotted decimal number representing the LSDB interface.
Age	Is a number representing the age of the link state advertisement in seconds.
Sequence	Is a number that represents which LSA is more recent.
Checksum	Is the total number LSA checksum.
Options	This is an integer. It indicates that the LSA receives special handling during routing calculations.
Rtr Opt	Router Options are valid for router links only.

show ipv6 ospf database database-summary

Use this command to display the number of each type of LSA in the database and the total number of LSAs in the database.

Format	**`show ipv6 ospf database database-summary`**
Modes	Privileged EXEC User EXEC

TABLE 5-15 Entry Definitions for `show ipv6 ospf database database-memory`

Entry	Definition
Router	Total number of router LSAs in the OSPFv3 link state database.
Network	Total number of network LSAs in the OSPFv3 link state database.
Inter-area Prefix	Total number of inter-area prefix LSAs in the OSPFv3 link state database.
Inter-area Router	Total number of inter-area router LSAs in the OSPFv3 link state database.
Type-7 Ext	Total number of NSSA external LSAs in the OSPFv3 link state database.
Link	Total number of link LSAs in the OSPFv3 link state database.
Intra-area Prefix	Total number of intra-area prefix LSAs in the OSPFv3 link state database.
Link Unknown	Total number of link-source unknown LSAs in the OSPFv3 link state database.
Area Unknown	Total number of area unknown LSAs in the OSPFv3 link state database.
AS Unknown	Total number of as unknown LSAs in the OSPFv3 link state database.
Type-5 Ext	Total number of AS external LSAs in the OSPFv3 link state database.
Self-Originated Type-5	Total number of self originated AS external LSAs in the OSPFv3 link state database.
Total	Total number of router LSAs in the OSPFv3 link state database.

show ipv6 ospf interface

This command displays the information for the IFO object or virtual interface tables.

Format	**`show ipv6 ospf interface`** *`{<slot/port> | loopback <loopback-id> | tunnel <tunnel-id>}`*
Modes	Privileged EXEC User EXEC

TABLE 5-16 Entry Definitions for `show ipv6 interface`

Entry	Definition
IP Address	Shows the IPv6 address of the interface.
ifIndex	Shows the interface index number associated with the interface.
OSPF Admin Mode	Shows whether the admin mode is enabled or disabled.
OSPF Area ID	Shows the area ID associated with this interface.
Router Priority	Shows the router priority. The router priority determines which router is the designated router.
Retransmit Interval	Shows the frequency, in seconds, at which the interface sends LSA.
Hello Interval	Shows the frequency, in seconds, at which the interface sends Hello packets.
Dead Interval	Shows the amount of time, in seconds, the interface waits before assuming a neighbor is down.
LSA Ack Interval	Shows the amount of time, in seconds, the interface waits before sending an LSA acknowledgement after receiving an LSA.
Iftransit Delay Interval	Shows the number of seconds the interface adds to the age of LSA packets before transmission.
Authentication Type	Shows the type of authentication the interface performs on LSAs it receives.
Metric Cost	Shows the priority of the path. Low costs have a higher priority than high costs.
OSPF MTU-ignore	Shows whether to ignore MTU mismatches in database descriptor packets sent from neighboring routers. The following information only displays if OSPF is initialized on the interface:
OSPF Interface Type	Broadcast LANs, such as Ethernet and IEEE 802.5, take the value *`broadcast`*. The OSPF Interface Type will be 'broadcast'.
State	The OSPF Interface States are: down, loopback, waiting, point-to-point, designated router, and backup designated router.

TABLE 5-16 Entry Definitions for `show ipv6 interface` *(Continued)*

Entry	Definition
Designated Router	The router ID representing the designated router.
Backup Designated Router	The router ID representing the backup designated router.
Number of Link Events	The number of link events.
Metric Cost	The cost of the OSPF interface.

show ipv6 ospf interface brief

This command displays brief information for the IFO object or virtual interface tables.

Format	**`show ipv6 ospf interface brief`**
Modes	Privileged EXEC User EXEC

TABLE 5-17 Entry Definitions for `show ipv6 interface brief`

Entry	Definition
Interface	Valid slot and port number separated by forward slashes.
OSPF Admin Mode	States whether OSPF is enabled or disabled on a router interface.
OSPF Area ID	Represents the OSPF Area ID for the specified interface.
Router Priority	Shows the router priority. The router priority determines which router is the designated router.
Hello Interval	Shows the frequency, in seconds, at which the interface sends Hello packets.
Dead Interval	Shows the amount of time, in seconds, the interface waits before assuming a neighbor is down.

TABLE 5-17 Entry Definitions for `show ipv6 interface brief` *(Continued)*

Entry	Definition
Retransmit Interval	Shows the frequency, in seconds, at which the interface sends LSA.
Retransmit Delay Interval	Shows the number of seconds the interface adds to the age of LSA packets before transmission.
LSA Ack Interval	Shows the amount of time, in seconds, the interface waits before sending an LSA acknowledgement after receiving an LSA.

show ipv6 ospf interface stats

This command displays the statistics for a specific interface. The command only displays information if OSPF is enabled.

Format	**`show ipv6 ospf interface stats`** *`<slot/port>`*
Modes	Privileged EXEC User EXEC

TABLE 5-18 Entry Definitions for `show ipv6 ospf interface stats`

Entry	Definition
OSPFv3 Area ID	The area id of this OSPF interface.
IP Address	The IP address associated with this OSPF interface.
OSPFv3 Interface Events	The number of times the specified OSPF interface has changed its state, or an error has occurred.
Virtual Events	The number of state changes or errors that occurred on this virtual link.
Neighbor Events	The number of times this neighbor relationship has changed state, or an error has occurred.
Packets Received	The number of OSPFv3 packets received on the interface.
Packets Transmitted	The number of OSPFv3 packets sent on the interface.
LSAs Sent	The total number of LSAs flooded on the interface.
LSA Acks Received	The total number of LSA acknowledged from this interface.
LSA Acks Sent	The total number of LSAs acknowledged to this interface.

show ipv6 ospf neighbor

This command displays information about OSPF neighbors. If you do not specify a neighbor IP address, the output displays summary information in a table. If you specify an interface or tunnel, only the information for that interface or tunnel displays. The *<ip-address>* is the IP address of the neighbor, and when you specify this, detailed information about the neighbor displays. The information below only displays if OSPF is enabled and the interface has a neighbor.

Format	**`show ipv6 ospf neighbor`** `[`*`interface`*` {<`*`slot/port`*`> | `*`tunnel`*` <`*`tunnel_id`*`>}][<`*`ip-address`*`>]`
Modes	Privileged EXEC User EXEC

If you do not specify an IP address, a table with the following columns displays for all neighbors or the neighbor associated with the interface that you specify.

TABLE 5-19 Entry Definitions for `show ipv6 ospf neighbor`

Entry	Definition
Router ID	Shows the 4-digit dotted-decimal number of the neighbor router.
Priority	Displays the OSPF priority for the specified interface. The priority of an interface is a priority integer from 0 to 255. A value of '0' indicates that the router is not eligible to become the designated router on this network.
Intf ID	Shows the interface ID of the neighbor.
Interface	Shows the interface of the local router in slot/port format.

TABLE 5-19 Entry Definitions for `show ipv6 ospf neighbor` *(Continued)*

Entry	Definition
State	Shows the state of the neighboring routers. Possible values are as follows: • Down- initial state of the neighbor conversation - no recent information has been received from the neighbor. • Attempt - no recent information has been received from the neighbor but a more concerted effort should be made to contact the neighbor. • Init - an Hello packet has recently been seen from the neighbor, but bidirectional communication has not yet been established. • 2 way - communication between the two routers is bidirectional. • Exchange start - the first step in creating an adjacency between the two neighboring routers, the goal is to decide which router is the master and to decide upon the initial DD sequence number. • Exchange - the router is describing its entire link state database by sending Database Description packets to the neighbor. • Loading - Link State Request packets are sent to the neighbor asking for the more recent LSAs that have been discovered (but not yet received) in the Exchange state. • Full - the neighboring routers are fully adjacent and they will now appear in router-LSAs and network-LSAs.
Dead Time	Shows the amount of time, in seconds, to wait before the router assumes the neighbor is unreachable. If you specify an IP address for the neighbor router, the following fields display:
Interface	Shows the interface of the local router in slot/port format.
Area ID	The area ID associated with the interface.
Options	An integer value that indicates the optional OSPF capabilities supported by the neighbor. These are listed in its Hello packets. This enables received Hello Packets to be rejected (i.e., neighbor relationships will not even start to form) if there is a mismatch in certain crucial OSPF capabilities.
Router Priority	Displays the router priority for the specified interface.
Dead Timer Due	Shows the amount of time, in seconds, to wait before the router assumes the neighbor is unreachable.
State	Shows the state of the neighboring routers.
Events	Number of times this neighbor relationship has changed state, or an error has occurred.
Retransmission Queue Length	Is an integer representing the current length of the retransmission queue of the specified neighbor router Id of the specified interface.

`show ipv6 ospf range`

This command displays information about the area ranges for the specified <*areaid*>. The <*areaid*> identifies the OSPF area whose ranges are being displayed.

Format	**`show ipv6 ospf range <`*`areaid`*`>`**
Modes	Privileged EXEC
User EXEC	

TABLE 5-20 Entry Definitions for `show ipv6 ospf range`

Entry	Definition
Area ID	The area id of the requested OSPF area.
IP Address	An IP Address which represents this area range.
Subnet Mask	A valid subnet mask for this area range.
Lsdb Type	The type of link advertisement associated with this area range.
Advertisement	The status of the advertisement: enabled or disabled.

`show ipv6 ospf stub table`

This command displays the OSPF stub table. The information below will only be displayed if OSPF is initialized on the switch.

Format	**`show ipv6 ospf stub table`**
Modes	Privileged EXEC User EXEC

TABLE 5-21 Entry Definitions for `show ipv6 ospf stub table`

Entry	Definition
Area ID	A 32-bit identifier for the created stub area.

TABLE 5-21 Entry Definitions for `show ipv6 ospf stub table` *(Continued)*

Entry	Definition
Type of Service	Type of service associated with the stub metric. For this release, Normal TOS is the only supported type.
Metric Val	The metric value is applied based on the TOS. It defaults to the least metric of the type of service among the interfaces to other areas. The OSPF cost for a route is a function of the metric value.
Import Summary LSA	Controls the import of summary LSAs into stub areas.

show ipv6 ospf virtual-link

This command displays the OSPF Virtual Interface information for a specific area and neighbor. The <*areaid*> parameter identifies the area and the <*neighbor*> parameter identifies the neighbor's Router ID.

Format	**show ipv6 ospf virtual-link <*areaid*> <*neighbor*>**
Modes	Privileged EXEC User EXEC

TABLE 5-22 Entry Definitions for `show ipv6 ospf virtual-link`

Entry	Definition
Area ID	The area id of the requested OSPF area.
Neighbor Router ID	The input neighbor Router ID.
Hello Interval	The configured hello interval for the OSPF virtual interface.
Dead Interval	The configured dead interval for the OSPF virtual interface.
Iftransit Delay Interval	The configured transit delay for the OSPF virtual interface.
Retransmit Interval	The configured retransmit interval for the OSPF virtual interface.
Authentication Type	Shows the type of authentication the interface performs on LSAs it receives.
State	The OSPF Interface States are: down, loopback, waiting, point-to-point, designated router, and backup designated router. This is the state of the OSPF interface.
Neighbor State	The neighbor state.

`show ipv6 ospf virtual-link brief`

This command displays the OSPFV3 Virtual Interface information for all areas in the system.

Format	**`show ipv6 ospf virtual-link brief`**
Mode	Privileged EXEC User EXEC

TABLE 5-23 Entry Definitions for `show ipv6 ospf virtual-link brief`

Entry	Definition
Area ID	The area id of the requested OSPFV3 area.
Neighbor	The neighbor interface of the OSPFV3 virtual interface.
Hello Interval	The configured hello interval for the OSPFV3 virtual interface.
Dead Interval	The configured dead interval for the OSPFV3 virtual interface.
Retransmit Interval	The configured retransmit interval for the OSPFV3 virtual interface.
Transit Delay	The configured transit delay for the OSPFV3 virtual interface.

DHCPv6 Commands

This section describes the command you use to configure the DHCPv6 server on the system and to view DHCPv6 information.

service dhcpv6

This command enables DHCPv6 configuration on the router.

Default	enabled
Format	**`service dhcpv6`**
Mode	Global Config

no service dhcpv6

This command disables DHCPv6 configuration on router.

Format	**`no service dhcpv6`**
Mode	Global Config

ipv6 dhcp server

Use this command to configure DHCPv6 server functionality on an interface. The *`<pool-name>`* is the DHCPv6 pool containing stateless and/or prefix delegation parameters, *`rapid-commit`* is an option that allows for an abbreviated exchange between the client and server, and *`<pref-value>`* is a value used by clients to determine preference between multiple DHCPv6 servers. For a particular interface DHCPv6 server and DHCPv6 relay functions are mutually exclusive.

Format	**`ipv6 dhcp server`** *`<pool-name> [rapid-commit] [preference <pref-value>]`*
Mode	Interface Config

ipv6 dhcp relay destination

Use this command to configure an interface for DHCPv6 relay functionality.

- Use the *destination* keyword to set the relay server IPv6 address. The *<relay-address>* parameter is an IPv6 address of a DHCPv6 relay server.
- Use the *interface* keyword to set the relay server interface. The *<relay-interface>* parameter is an interface (slot/port) to reach a relay server. The optional *remote-id* is the Relay Agent Information Option "remote ID" sub-option to be added to relayed messages. This can either be the special keyword *duid-ifid*, which causes the "remote ID" to be derived from the DHCPv6 server DUID and the relay interface number, or it can be specified as a user-defined string.

Note – If *<relay-address>* is an IPv6 global address, then *<relay-interface>* is not required. If *<relay-address>* is a link-local or multicast address, then *<relay-interface>* is required. Finally, if you do not specify a value for *<relay-address>*, then you must specify a value for *<relay-interface>* and the DHCPV6-ALL-AGENTS multicast address (i.e. FF02::1:2) is used to relay DHCPv6 messages to the relay server.

Format	**ipv6 dhcp relay** *{destination [<relay-address>] interface [<relay-interface>]| interface [<relay-interface>]} [remote-id (duid-ifid | <user-defined-string>)]*
Mode	Interface Config

ipv6 dhcp relay-agent-info-opt

Use this command to configure a number to represent the DHCPv6 Relay Agent Information Option. The DHCPv6 Relay Agent Information Option allows for various sub-options to be attached to messages that are being relayed by the local router to a relay server. The relay server may in turn use this information in determining an address to assign to a DHCPv6 client.

Default	32
Format	**ipv6 dhcp relay-agent-info-opt** *<32-65535>*
Mode	Global Config

ipv6 dhcp relay-agent-info-remote-id-subopt

Use this command to configure a number to represent the DHCPv6 the “remote-id” sub-option.

Default	1
Format	**`ipv6 dhcp relay-agent-info-remote-id-subopt`** *`<1-65535>`*
Mode	Global Config

ipv6 dhcp pool

Use this command from Global Config mode to enter IPv6 DHCP Pool Config mode. Use the **`exit`** command to return to Global Config mode. To return to the User EXEC mode, enter CTRL+Z. The *`<pool-name>`* should be less than 31 alpha-numeric characters. DHCPv6 pools are used to specify information for DHCPv6 server to distribute to DHCPv6 clients. These pools are shared between multiple interfaces over which DHCPv6 server capabilities are configured.

Format	**`ipv6 dhcp pool`** *`<pool-name>`*
Mode	Global Config

no ipv6 dhcp pool

This command removes the specified DHCPv6 pool.

Format	**`no ipv6 dhcp pool`** *`<pool-name>`*
Mode	Global Config

domain-name (IPv6)

This command sets the DNS domain name which is provided to DHCPv6 client by DHCPv6 server. DNS domain name is configured for stateless server support. Domain name consist of no more than 31 alpha-numeric characters. DHCPv6 pool can have multiple number of domain names with maximum of 8.

Format	**`domain-name`** *`<dns-domain-name>`*
Mode	IPv6 DHCP Pool Config

no domain-name

This command will remove dhcpv6 domain name from dhcpv6 pool.

Format	**`no domain-name`** *`<dns-domain-name>`*
Mode	IPv6 DHCP Pool Config

dns-server (IPv6)

This command sets the ipv6 DNS server address which is provided to dhcpv6 client by dhcpv6 server. DNS server address is configured for stateless server support. DHCPv6 pool can have multiple number of domain names with maximum of 8.

Format	**`dns-server`** *`<dns-server-address>`*
Mode	IPv6 DHCP Pool Config

no dns-server

This command will remove DHCPv6 server address from DHCPv6 server.

Format	**`no dns-server`** *`<dns-server-address>`*
Mode	IPv6 DHCP Pool Config

prefix-delegation (IPv6)

Multiple IPv6 prefixes can be defined within a pool for distributing to specific DHCPv6 Prefix delegation clients. Prefix is the delegated IPv6 prefix. DUID is the client's unique DUID value (Example: 00:01:00:09:f8:79:4e:00:04:76:73:43:76'). Name is 31 characters textual client's name which is useful for logging or tracing only. Valid lifetime is the valid lifetime for the delegated prefix in seconds and preferred lifetime is the preferred lifetime for the delegated prefix in seconds.

Default	preferred-lifetime: 2592000 valid-lifetime: 604800
Format	**`prefix-delegation`** *`<prefix/prefixlength> <DUID> [name <hostname>] [valid-lifetime <04294967295>][preferred-lifetime < 0-4294967295>]`*
Mode	IPv6 DHCP Pool Config

no prefix-delegation

This command deletes a specific prefix-delegation client.

Format	**`no prefix-delegation`** *`<prefix/prefix-delegation> <DUID>`*
Mode	IPv6 DHCP Pool Config

show ipv6 dhcp

This command displays the DHCPv6 server name and status.

Format	**`show ipv6 dhcp`**
Mode	Privileged EXEC
DHCPv6 is Enabled (Disabled)	Shows the status of the DHCPv6 server.
Server DUID:	If configured, shows the DHCPv6 unique identifier

show ipv6 dhcp statistics

This command displays the IPv6 DHCP statistics for all interfaces.

Format	**`show ipv6 dhcp statistics`**
Mode	Privileged EXEC

TABLE 5-24 Entry Definitions for `show ipv6 dhcp statistics`

Entry	Definition
DHCPv6 Solicit Packets Received	Number of solicit received statistics.
DHCPv6 Request Packets Received	Number of request received statistics.
DHCPv6 Confirm Packets Received	Number of confirm received statistics.
DHCPv6 Renew Packets Received	Number of renew received statistics.
DHCPv6 Rebind Packets Received	Number of rebind received statistics.
DHCPv6 Release Packets Received	Number of release received statistics.
DHCPv6 Decline Packets Received	Number of decline received statistics.
DHCPv6 Inform Packets Received	Number of inform received statistics.
DHCPv6 Relay-forward Packets Received	Number of relay forward received statistics.
DHCPv6 Relay-reply Packets Received	Number of relay-reply received statistics.
DHCPv6 Malformed Packets Received	Number of malformed packets statistics.
Received DHCPv6 Packets Discarded	Number of DHCP discarded statistics.

TABLE 5-24 Entry Definitions for `show ipv6 dhcp statistics` *(Continued)*

Entry	Definition
Total DHCPv6 Packets Received	Total number of DHCPv6 received statistics.
DHCPv6 Advertisement Packets Transmitted	Number of advertise sent statistics.
DHCPv6 Reply Packets Transmitted	Number of reply sent statistics.
DHCPv6 Reconfig Packets Transmitted	Number of reconfigure sent statistics.
DHCPv6 Relay-reply Packets Transmitted	Number of relay-reply sent statistics.
DHCPv6 Relay-forward Packets Transmitted	Number of relay-forward sent statistics.
Total DHCPv6 Packets Transmitted	total number of DHCPv6 sent statistics.

show ipv6 dhcp interface

This command displays DHCPv6 information for all relevant interfaces or the specified interface. If you specify an interface, you can use the optional *statistics* parameter to view statistics for the specified interface.

Format	**`show ipv6 dhcp interface`** *`<slot/port> [statistics]`*
Mode	Privileged EXEC

TABLE 5-25 Entry Definitions for `show ipv6 dhcp interface`

Entry	Definition
IPv6 Interface	Shows the interface name in *`<slot/port>`* format.
Mode	Shows whether the interface is a IPv6 DHCP relay or server.
(Server)	If the interface mode is server, the following information displays.

TABLE 5-25 Entry Definitions for `show ipv6 dhcp interface` *(Continued)*

Entry	Definition
Pool Name	Shows the pool name specifying information for DHCPv6 server distribution to DHCPv6 clients.
Server Preference	Shows the preference of the server.
Option Flags	Shows whether rapid commit is enabled..
(Relay)	If the interface mode is relay, the following information displays
Relay Address	Shows the IPv6 address of the relay server.
Relay Interface Number	Shows the relay server interface in *<slot/port>* format.
Relay Remote ID	If configured, shows the name of the relay remote.
Option Flags	Shows whether rapid commit is configured.

If you use the statistics parameter, the command displays the IPv6 DHCP statistics for the specified interface. See "show ipv6 dhcp statistics" on page 313 for information about the output.

clear ipv6 dhcp

Use this command to clear DHCPv6 statistics for all interfaces or for a specific interface. Use the *<slot/port>* parameter to specify the interface.

Format	**`clear ipv6 dhcp`** *`{statistics	interface <slot/port> statistics}`*
Mode	Privileged EXEC

show ipv6 dhcp pool

This command displays configured DHCP pool.

Format	**`show ipv6 dhcp pool`** *`<pool-name>`*
Mode	Privileged EXEC

TABLE 5-26 Entry Definitions for `show ipv6 dhcp pool`

Entry	Definition
DHCP Pool Name	Unique pool name configuration.
Client DUID	Client's DHCP unique identifier. DUID is generated using the combination of the local system burned-in MAC address and a timestamp value.
Host	Name of the client.
Prefix/Prefix Length	IPv6 address and mask length for delegated prefix.
Preferred Lifetime	Preferred lifetime in seconds for delegated prefix.
Valid Lifetime	Valid lifetime in seconds for delegated prefix.
DNS Server Address	Address of DNS server address.
Domain Name	DNS domain name.

`show ipv6 dhcp binding`

This command displays configured DHCP pool.

Format	**`show ipv6 dhcp binding`** *`[<ipv6-address>]`*
Mode	Privileged EXEC

TABLE 5-27 Entry Definitions for `show ipv6 dhcp interface`

Entry	Definition
DHCP Client Address	Address of DHCP Client
DUID	String that represents the Client DUID.
IAID	Identity Association ID
Prefix/Prefix Length	IPv6 address and mask length for delegated prefix.
Prefix Type	IPV6 Prefix type (IAPD, IANA, or IATA).
Client Address	Address of DHCP Client.
Client Interface	IPv6 Address of DHCP Client.
Expiration	Address of DNS server address.
Valid Lifetime	Valid lifetime in seconds for delegated prefix.
Preferred Lifetime	Preferred lifetime in seconds for delegated prefix.

CHAPTER 6

IP Multicast Commands

This chapter describes the IP Multicast commands available in the FASTPATH® CLI.

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

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

This chapter contains the following sections:

Multicast Commands

This section describes the commands you use to configure IP Multicast and to view IP Multicast settings and statistics.

`ip mcast boundary`

This command adds an administrative scope multicast boundary specified by <*groupipaddr*> and <*mask*> for which this multicast administrative boundary is applicable. <*groupipaddr*> is a group IP address and <*mask*> is a group IP mask.

Format	**`ip mcast boundary`** **<***groupipaddr***>** **<mask>**
Mode	Interface Config

`no ip mcast boundary`

This command deletes an administrative scope multicast boundary specified by <*groupipaddr*> and <*mask*> for which this multicast administrative boundary is applicable. <*groupipaddr*> is a group IP address and <*mask*> is a group IP mask.

Format	**`no ip mcast boundary`** **<***groupipaddr***>** **<***mask***>**
Mode	Interface Config

ip multicast

This command sets the administrative mode of the IP multicast forwarder in the router to active. For multicast routing to become operational, IGMP must be currently enabled. An error message will be displayed on the CLI if multicast routing is enabled while IGMP is disabled. However, the IP multicast mode configuration is stored in the multicast configuration file and is automatically enabled once IGMP is enabled.

Default	disabled
Format	**`ip multicast`**
Mode	Global Config

no ip multicast

This command sets the administrative mode of the IP multicast forwarder in the router to inactive. For multicast routing to become operational, IGMP must be currently enabled. An error message will be displayed on the CLI if multicast routing is enabled while IGMP is disabled. However, the IP multicast mode configuration is stored in the multicast configuration file and is automatically enabled once IGMP is enabled.

Format	**`no ip multicast`**
Mode	Global Config

ip multicast staticroute

This command creates a static route which is used to perform RPF checking in multicast packet forwarding. The combination of the <*`sourceipaddr`*> and the <*`mask`*> fields specify the network IP address of the multicast packet source. The <*`rpfipaddr`*> is the IP address of the next hop toward the source. The <*`metric`*> is the cost of the route entry for comparison with other routes to the source network and is a value in the range of 0 and 255. The `current` incoming interface is used for RPF checking for multicast packets matching this multicast static route entry.

Default	none
Format	**`ip multicast staticroute`** *`<sourceipaddr> <mask> <rpfipaddr> <metric> <slot/port>`*
Mode	Global Config

`no ip multicast staticroute`

This command add deletes a static route in the static mcast table. The *`<sourceipaddr>`* is the IP address of the multicast packet source.

Format	**`no ip multicast staticroute <`***`sourceipaddr`***`>`**
Mode	Global Config

`ip multicast ttl-threshold`

This command applies the given *`<ttlthreshold>`* to a routing interface. The *`<ttlthreshold>`* is the TTL threshold which is to be applied to the multicast Data packets which are to be forwarded from the interface. The value for *`<ttlthreshold>`* has range from 0 to 255.

Default	1
Format	**`ip multicast ttl-threshold <`***`ttlvalue`***`>`**
Mode	Interface Config

no ip multicast ttl-threshold

This command applies the default <*ttlthreshold*> to a routing interface. The <*ttlthreshold*> is the TTL threshold which is to be applied to the multicast Data packets which are to be forwarded from the interface.

Format	**`no ip multicast ttl-threshold`**
Mode	Interface Config

disable ip multicast mdebug mtrace

This command is used to disable the processing capability of mtrace query on this router. If the mode is enable, the mtrace queries received by the router are processed and forwarded appropriately by the router. If the mode is disable, this router does not respond to the mtrace queries it receives from other router devices.

Default	none
Format	**`disable ip multicast mdebug mtrace`**
Mode	Global Config

no disable ip multicast mdebug mtrace

This command is used to enable the processing capability of mtrace query on this router. If the mode is enable, the mtrace queries received by the router are processed and forwarded appropriately by the router. If the mode is disable, this router does not respond to the mtrace queries it receives from other router devices.

Format	**`no disable ip multicast mdebug mtrace`**
Mode	Global Config

`mrinfo`

This command is used to query the neighbor information of a multicast-capable router specified by *`[ipaddr]`*. The default value is the IP address of the system at which the command is issued. The mrinfo command can take up to 2 minutes to complete. Only one mrinfo command may be in process at a time. The results of this command will be available in the results bufferpool which can be displayed by using **`show mrinfo`**.

Format	**`mrinfo`** *`[<ipaddr>]`*
Mode	Privileged EXEC

`mstat`

Use this command to find the IP Multicast packet rate and loss information path from a source to a receiver (unicast router id of the host running mstat). The results of this command are available in the results bufferpool which you can display by using the command "show mstat" on page 332. If a debug command is already in progress, a message is displayed and the new request fails.

The <*`source`*> is the IP address of the remote multicast-capable source. The [*`receiver`*] is the IP address of the receiver. The default value is the IP address of the system at which the command is issued. The [*`group`*] is a multicast address of the group to be displayed. The default value is 224.2.0.1(the group used for the multicast backbone).

Note – You can enter the group and receiver IP addresses in any order.

Default	none
Format	**`mstat`** *`<source> [<group/receiver>] [<group/receiver>]`*
Mode	Privileged EXEC

mtrace

This command is used to find the IP Multicast path from a source to a receiver (unicast router ID of the host running mtrace). A trace query is passed hop-by-hop along the reverse path from the receiver to the source, collecting hop addresses, packet counts, and routing error conditions along the path, and then the response is returned to the requestor. The results of this command are available in the results buffer pool which can be displayed by using the command "show mtrace" on page 332.

The <*source*> is the IP address of the remote multicast-capable source. The *[receiver]* is the IP address of the receiver. The default value is the IP address of system at which the command is issued. The *[group]* is the multicast address of the group to be displayed. The default value is 224.2.0.1(the group used for the multicast backbone). If a debug command is already in execution, a message is displayed and the new request fails.

Note – You can enter the group and destination IP addresses in any order.

Default	none
Format	**mtrace** *<sourceipaddr> [<group/destination>] [<group/destination >]*
Mode	Privileged EXEC

no ip mcast mroute

Use this command to clear entries in the mroute table. Use the *all* parameter to clear all entries. Use the *source* parameter to clear the routes in the mroute table entries containing the specified *<sourceipaddr>* or *<sourceipaddr> [groupipaddr]* pair. The source address is the source IP address of the multicast packet. The group address is the Group Destination IP address of the multicast packet. Use the *group* parameter to clear the routes in the mroute table entries containing the specified <*groupipaddr*>. The group address is the Group Destination IP address of the multicast packet.

Default	none
Format	**no ip mcast mroute** *{group <groupipaddr> | source <sourceipaddr> [<groupipaddr>] | all}*
Mode	Global Config

`show ip mcast`

This command displays the system-wide multicast information.

Format	**`show ip mcast`**
Modes	Privileged EXEC User EXEC

TABLE 6-1 Entry Definitions for `show ip mcast`

Entry	Definition
Admin Mode	The administrative status of multicast.
Protocol State	The current state of the multicast protocol. Possible values are Operational or Non-Operational.
Table Max Size	The maximum number of entries allowed in the multicast table.
Number Of Packets For Which Source Not Found	The number of packets for which the source is not found.
Number Of Packets For Which Group Not Found	The number of packets for which the group is not found.
Protocol	The multicast protocol running on the router. Possible values are PIMDM, PIMSM, or DVMRP.
Entry Count	The number of entries in the multicast table.
Highest Entry Count	The highest entry count in the multicast table.

show ip mcast boundary

This command displays all the configured administrative scoped multicast boundaries.

Format	**`show ip mcast boundary`** *`{<slot/port> | all}`*
Modes	Privileged EXEC User EXEC
Interface	Valid slot and port number separated by forward slashes.
Group Ip	The group IP address
Mask	The group IP mask

show ip mcast interface

This command displays the multicast information for the specified interface.

Format	**`show ip mcast interface`** *`<slot/port>`*
Modes	Privileged EXEC User EXEC
Interface	Valid slot and port number separated by forward slashes.
TTL	The time-to-live value for this interface.

show ip mcast mroute

This command displays a summary or all the details of the multicast table.

Format	**`show ip mcast mroute`** *`{detail	summary}`*
Modes	Privileged EXEC User EXEC

TABLE 6-2 Entry Definitions for `show ip mcast mroute`

Entry	Definition
Source IP Addr	The IP address of the multicast data source.
Group IP Addr	The IP address of the destination of the multicast packet.
Expiry Time	The time of expiry of this entry in seconds.
Up Time	The time elapsed since the entry was created in seconds.
RPF Neighbor	The IP address of the RPF neighbor.
Flags	The flags associated with this entry.
	If you use the *`summary`* parameter, the command displays the following fields.
Source IP Addr	The IP address of the multicast data source.
Group IP Addr	The IP address of the destination of the multicast packet.
Protocol	The multicast routing protocol by which the entry was created.
Incoming Interface	The interface on which the packet for the source/group arrives.
Outgoing Interface List	The list of outgoing interfaces on which the packet is forwarded.

show ip mcast mroute group

This command displays the multicast configuration settings such as flags, timer settings, incoming and outgoing interfaces, RPF neighboring routers, and expiration times of all the entries in the multicast mroute table containing the given *<groupipaddr>*.

Format	**`show ip mcast mroute group`** *`<groupipaddr> {detail |summary}`*
Modes	Privileged EXEC User EXEC

TABLE 6-3 Entry Definitions for `show ip mcast mroute` group

Entry	**Definition**
Source IP Addr	The IP address of the multicast data source.
Group IP Addr	The IP address of the destination of the multicast packet.
Protocol	The multicast routing protocol by which this entry was created.
Incoming Interface	The interface on which the packet for this group arrives.
Outgoing Interface List	The list of outgoing interfaces on which this packet is forwarded.

show ip mcast mroute source

This command displays the multicast configuration settings such as flags, timer settings, incoming and outgoing interfaces, RPF neighboring routers, and expiration times of all the entries in the multicast mroute table containing the given source IP address or source IP address and group IP address pair.

Format	**`show ip mcast mroute source`** *`<sourceipaddr> {summary	<groupipaddr>}`*
Modes	Privileged EXEC User EXEC

If you use the *`<groupipaddr>`* parameter, the command displays the following column headings in the output table.

TABLE 6-4 Entry Definitions for `show ip mcast mroute` source group

Entry	Definition
Source IP Addr	The IP address of the multicast data source.
Group IP Addr	The IP address of the destination of the multicast packet.
Expiry Time	The time of expiry of this entry in seconds.
Up Time	The time elapsed since the entry was created in seconds.
RPF Neighbor	The IP address of the RPF neighbor.
Flags	The flags associated with this entry.

If you use the *`summary`* parameter, the command displays the following column headings in the output table.

TABLE 6-5 Entry Definitions for `show ip mcast mroute` source summary

Entry	Definition
Source IP Addr	The IP address of the multicast data source.
Group IP Addr	The IP address of the destination of the multicast packet.
Protocol	The multicast routing protocol by which this entry was created.
Incoming Interface	The interface on which the packet for this source arrives.
Outgoing Interface List	The list of outgoing interfaces on which this packet is forwarded.

show ip mcast mroute static

This command displays all the static routes configured in the static mcast table if is specified or displays the static route associated with the particular <*sourceipaddr*>.

Format	**show ip mcast mroute static** *[<sourceipaddr>]*
Modes	Privileged EXEC User EXEC

TABLE 6-6 Entry Definitions for `show ip mcast mroute` static

Entry	Definition
Source Address	The IP address of the multicast packet source.
Source Mask	The mask applied to the IP address of the multicast packet source.
RPF Address	The IP address to be used as RPF for the given source and mask.
Metric	The metric value corresponding to the source address.
Interface	Valid slot and port number separated by forward slashes.

show mrinfo

This command is used to display the neighbor information of a multicast-capable router from the results buffer pool of the router subsequent to the execution/completion of a **mrinfo** *[ipaddr]* command. The results subsequent to the completion of the latest **mrinfo** will be available in the buffer pool after a maximum duration of two minutes after the completion of the **show mrinfo** command. A subsequent issue **mrinfo** overwrites the contents of the buffer pool with fresh results.

Default	none
Format	**show mrinfo**
Mode	Privileged EXEC

TABLE 6-7 Entry Definitions for `show mrinfo`

Entry	Definition
Router Interface	The IP address of this neighbor
Neighbor	The neighbor associated with the router interface

TABLE 6-7 Entry Definitions for `show mrinfo`

Entry	Definition
Metric	The metric value associated with this neighbor
TTL	The TTL threshold associated with this neighbor
Flags	Status of the neighbor

`show mstat`

This command is used to display the results of packet rate and loss information from the results buffer pool of the router, subsequent to the execution/completion of a **`mstat`** *`<source> [group] [receiver]`* command. Within two minutes of the completion of the **`mstat`** command, the results will be available in the buffer pool. The next issuing of **`mstat`** overwrites the buffer pool with fresh results.

Default	none
Format	show mstat
Mode	Privileged EXEC

`show mtrace`

This command is used to display results of multicast trace path from the results buffer pool of the router, subsequent to the execution/completion of a **`mtrace`** *`<source> [group] [receiver]`* command. The results subsequent to the completion of the **`mtrace`** will be available in the buffer pool within two minutes and thereafter. A subsequent **`mtrace`** command overwrites the results in the buffer pool.

Default	none
Format	**`show mtrace`**
Modes	Privileged EXEC User EXEC

TABLE 6-8 Entry Definitions for `show mrtrace`

Entry	Definition
Hops Away From Destination	The ordering of intermediate routers between the source and the destination
Intermediate Router Address	The address of the intermediate router at the specified hop distance
Mcast Protocol In Use	The multicast routing protocol used for the out interface of the specified intermediate router.
TTL Threshold	The Time-To-Live threshold of the out interface on the specified intermediate router.
Time Elapsed Between Hops (msecs)	The time between arrival at one intermediate router to the arrival at the next.

DVMRP Commands

This section provides a detailed explanation of the Distance Vector Multicast Routing Protocol (DVMRP) commands.

`ip dvmrp`

This command sets administrative mode of DVMRP in the router to active. IGMP must be enabled before DVMRP can be enabled.

Default	disabled
Format	**`ip dvmrp`**
Mode	Global Config

`no ip dvmrp`

This command sets administrative mode of DVMRP in the router to inactive.

Format	**`no ip dvmrp`**
Mode	Global Config

`ip dvmrp metric`

This command configures the metric for an interface. This value is used in the DVMRP messages as the cost to reach this network. This field has a range of 1 to 31.

Default	1
Format	ip dvmrp metric <*`metric`*>
Mode	Interface Config

`no ip dvmrp metric`

This command resets the metric for an interface to the default value. This value is used in the DVMRP messages as the cost to reach this network.

Format	no ip dvmrp metric
Mode	Interface Config

`ip dvmrp trapflags`

This command enables the DVMRP trap mode.

Default	disabled
Format	*`ip dvmrp trapflags`*
Mode	Global Config

`no ip dvmrp trapflags`

This command disables the DVMRP trap mode.

Format	*`no ip dvmrp trapflags`*
Mode	Global Config

`ip dvmrp`

This command sets the administrative mode of DVMRP on an interface to active.

Default	disabled
Format	**`ip dvmrp`**
Mode	Interface Config

`no ip dvmrp`

This command sets the administrative mode of DVMRP on an interface to inactive.

Format	**`no ip dvmrp`**
Mode	Interface Config

show ip dvmrp

This command displays the system-wide information for DVMRP.

Format	**`show ip dvmrp`**
Modes	Privileged EXEC User EXEC

TABLE 6-9 Entry Definitions for `show ip dvmrp`

Entry	Definition
Admin Mode	This field indicates whether DVMRP is enabled or disabled.
Version String	The version of DVMRP being used.
Number of Routes	The number of routes in the DVMRP routing table.
Reachable Routes	The number of entries in the routing table with non-infinite metrics. The following fields are displayed for each interface.
Interface	Valid slot and port number separated by forward slashes.
Interface Mode	The mode of this interface. Possible values are Enabled and Disabled.
State	The current state of DVMRP on this interface. Possible values are Operational or Non-Operational.

show ip dvmrp interface

This command displays the interface information for DVMRP on the specified interface.

Format	**`show ip dvmrp interface`** <*slot/port*>
Modes	Privileged EXEC User EXEC

TABLE 6-10 Entry Definitions for `show ip dvmrp interface`

Entry	Definition
Interface Mode	This field indicates whether DVMRP is enabled or disabled on the specified interface.
Metric	The metric of this interface. This is a configured value.
Local Address	The IP Address of the interface.

TABLE 6-10 Entry Definitions for `show ip dvmrp interface`

Entry	Definition
Generation ID	This field is displayed only when DVMRP is operational on the interface. The Generation ID value for the interface. This is used by the neighboring routers to detect that the DVMRP table should be resent. The following fields are displayed only if DVMRP is enabled on this interface.
Received Bad Packets	The number of invalid packets received.
Received Bad Routes	The number of invalid routes received.
Sent Routes	The number of routes that have been sent on this interface.

show ip dvmrp neighbor

This command displays the neighbor information for DVMRP.

Format	**`show ip dvmrp neighbor`**
Modes	Privileged EXEC User EXEC

TABLE 6-11 Entry Definitions for `show ip dvmrp neighbor`

Entry	Definition
IfIndex	The value of the interface used to reach the neighbor.
Nbr IP Addr	The IP Address of the DVMRP neighbor for which this entry contains information.
State	The state of the neighboring router. The possible value for this field are ACTIVE or DOWN.
Up Time	The time since this neighboring router was learned.
Expiry Time	The time remaining for the neighbor to age out. This field is not applicable if the State is DOWN.
Generation ID	The Generation ID value for the neighbor.
Major Version	The major version of DVMRP protocol of neighbor.
Minor Version	The minor version of DVMRP protocol of neighbor.
Capabilities	The capabilities of neighbor.

TABLE 6-11 Entry Definitions for `show ip dvmrp neighbor`

Entry	Definition
Received Routes	The number of routes received from the neighbor.
Rcvd Bad Pkts	The number of invalid packets received from this neighbor.
Rcvd Bad Routes	The number of correct packets received with invalid routes.

show ip dvmrp nexthop

This command displays the next hop information on outgoing interfaces for routing multicast datagrams.

Format	**`show ip dvmrp nexthop`**
Modes	Privileged EXEC User EXEC

TABLE 6-12 Entry Definitions for `show ip dvmrp nexthop`

Entry	Definition
Source IP	The sources for which this entry specifies a next hop on an outgoing interface.
Source Mask	The IP Mask for the sources for which this entry specifies a next hop on an outgoing interface.
Next Hop Interface	The interface in slot/port format for the outgoing interface for this next hop.
Type	The network is a LEAF or a BRANCH.

show ip dvmrp prune

This command displays the table listing the router′s upstream prune information.

Format	**`show ip dvmrp prune`**
Modes	Privileged EXEC User EXEC

TABLE 6-13 Entry Definitions for `show ip dvmrp prune`

Entry	Definition
Group IP	This field identifies the multicast Address that is pruned.
Source IP	This field displays the IP Address of the source that has pruned.
Source Mask	This field displays the network Mask for the prune source. It should be all 1s or both the prune source and prune mask must match.
Expiry Time (secs)	This field indicates the expiry time in seconds. This is the time remaining for this prune to age out.

show ip dvmrp route

This command displays the multicast routing information for DVMRP.

Format	**`show ip dvmrp route`**
Modes	Privileged EXEC User EXEC

TABLE 6-14 Entry Definitions for `show ip dvmrp route`

Entry	Definition
Source Address	This field displays the multicast address of the source group.
Source Mask	This field displays the IP Mask for the source group.
Upstream Neighbor	This field indicates the IP Address of the neighbor which is the source for the packets for a specified multicast address.
Interface	This field displays the interface used to receive the packets sent by the sources.

TABLE 6-14 Entry Definitions for `show ip dvmrp route`

Entry	Definition
Metric	This field displays the distance in hops to the source subnet. This field has a different meaning than the Interface Metric field.
Expiry Time (secs)	This field indicates the expiry time in seconds. This is the time remaining for this route to age out.
Up Time (secs)	This field indicates the time when a specified route was learnt, in seconds.

PIM-DM Commands

This section describes the commands you use to configure Protocol Independent Multicast - Dense Mode (PIM-DM). PIM-DM is a multicast routing protocol that provides scalable inter-domain multicast routing across the Internet, independent of the mechanisms provided by any particular unicast routing protocol. PIM-DM is typically used in LAN applications, while PIM-SM is for WAN applications.

`ip pimdm`

This command enables the administrative mode of PIM-DM in the router.

Default	disabled
Format	**`ip pimdm`**
Mode	Global Config

`no ip pimdm`

This command disables the administrative mode of PIM-DM in the router. IGMP must be enabled before PIM-DM can be enabled.

Format	**`no ip pimdm`**
Mode	Global Config

ip pimdm mode

This command sets administrative mode of PIM-DM on an interface to enabled.

Default	disabled
Format	**`ip pimdm mode`** *<slot/port>*
Mode	Interface Config

no ip pimdm mode

This command sets administrative mode of PIM-DM on an interface to disabled.

Format	**`no ip pimdm mode`** *<slot/port>*
Mode	Interface Config

ip pimdm query-interval

This command configures the transmission frequency of hello messages between PIM enabled neighbors. This field has a range of 10 to 3600 seconds.

Default	30
Format	**`ip pimdm query-interval`** *<seconds>*
Mode	Interface Config

no ip pimdm query-interval

This command resets the transmission frequency of hello messages between PIM enabled neighbors to the default value.

Format	**`no ip pimdm query-interval`**
Mode	Interface Config

`show ip pimdm`

This command displays the system-wide information for PIM-DM.

Format	**`show ip pimdm`**
Modes	Privileged EXEC User EXEC

TABLE 6-15 Entry Definitions for `show ip pimdm`

Entry	Definition
PIM-DM Admin Mode	This field indicates whether PIM-DM is enabled or disabled.
Interface	Valid slot and port number separated by forward slashes.
Interface Mode	This field indicates whether PIM-DM is enabled or disabled on this interface.
State	The current state of PIM-DM on this interface. Possible values are Operational or Non-Operational.

`show ip pimdm interface`

This command displays the interface information for PIM-DM on the specified interface.

Format	**`show ip pimdm interface`** *`<slot/port>`*
Modes	Privileged EXEC User EXEC
Interface Mode	This field indicates whether PIM-DM is enabled or disabled on the specified interface.
PIM-DM Interface Hello Interval	The frequency at which PIM hello messages are transmitted on this interface. By default, the value is 30 seconds.

`show ip pimdm interface stats`

This command displays the statistical information for PIM-DM on the specified interface.

Format	**`show ip pimdm interface stats`** *`{<slot/port>	all}`*
Modes	Privileged EXEC User EXEC

TABLE 6-16 Entry Definitions for `show ip pimdm interface stats`

Entry	Definition
Interface	Valid slot and port number separated by forward slashes.
IP Address	The IP Address that represents the PIM-DM interface.
Nbr Count	The neighbor count for the PIM-DM interface.
Hello Interval	The time interval between two hello messages sent from the router on the given interface.
Designated Router	The IP Address of the Designated Router for this interface.

`show ip pimdm neighbor`

This command displays the neighbor information for PIM-DM on the specified interface.

Format	**`show ip pimdm neighbor`** *`{<slot/port>	all}`*
Modes	Privileged EXEC User EXEC

TABLE 6-17 Entry Definitions for `show ip pimdm neighbor`

Entry	Definition
Neighbor Address	The IP Address of the neighbor on an interface.
Interface	Valid slot and port number separated by forward slashes.
Up Time	The time since this neighbor has become active on this interface.
Expiry Time	The expiry time of the neighbor on this interface.

PIM-SM Commands

This section describes the commands you use to configure Protocol Independent Multicast - Sparse Mode (PIM-SM). PIM-SM is a multicast routing protocol that provides scalable inter-domain multicast routing across the Internet, independent of the mechanisms provided by any particular unicast routing protocol. PIM-DM is typically used in LAN applications, while PIM-SM is for WAN applications.

ip pimsm cbsrpreference

This command is used to configure the CBSR preference for a particular PIM-SM interface. The range of CBSR preference is –1 to 255.

Default	0
Format	**`ip pimsm cbsrpreference`** *<-1-255>*
Mode	Interface Config

no ip pimsm cbsrpreference

Use this command to reset the CBSR preference for a particular PIM-SM interface to zero.

Format	no ip pimsm cbsrpreference
Mode	Interface Config

ip pimsm cbsrhashmasklength

This command is used to configure the CBSR hash mask length to be advertised in bootstrap messages for a particular PIM-SM interface. This hash mask length will be used in the hash algorithm for selecting the RP for a particular group. The valid range is 0 - 32.

Default	30
Format	**`ip pimsm cbsrhashmasklength`** *`<0-32>`*
Mode	Interface Config

no ip pimsm cbsrhashmasklength

Use this command to reset the CBSR hash mask length for a particular PIM-SM interface to the default.

Format	no ip pimsm **`cbsrhashmasklength`**
Mode	Interface Config

ip pimsm crppreference

This command is used to configure the Candidate Rendezvous Point (CRP) for a particular PIM-SM interface. The valid values are from (-1 to 255), and the value of -1 is used to indicate that the local interface is not a Candidate RP interface.

The active router interface, with the highest IP Address and crppreference greater than -1, is chosen as the CRP for the router. The default value is 0.

In the CRP advertisements sent to the bootstrap router (BSR), the router interface advertises itself as the CRP for the group range 224.0.0.0 mask 240.0.0.0.

Default	0
Format	**`ip pimsm crppreference`** *`<-1-255>`*
Mode	Interface Config

no ip pimsm crppreference

This command is used to reset the Candidate Rendezvous Point (CRP) for a particular PIM-SM interface to the default value.

Format	no ip pimsm **`crppreference`**
Mode	Interface Config

ip pimsm message-interval

This command is used to configure the global join/prune interval for PIM-SM router. The join/prune interval is specified in seconds. This parameter can be configured to a value from 10 to 3600.

Default	60
Format	**`ip pimsm message-interval`** *`<10-3600>`*
Mode	Global Config

no ip pimsm message-interval

Use this command to reset the global join/prune interval to the default value.

Format	**`no ip pimsm message-interval`**
Mode	Global Config

ip pimsm

This command sets administrative mode of PIM-SM multicast routing across the router to enabled. IGMP must be enabled before PIM-SM can be enabled.

Default	disabled
Format	**`ip pimsm`**
Mode	Global Config

no ip pimsm

This command sets administrative mode of PIM-SM multicast routing across the router to the default value. IGMP must be enabled before PIM-SM can be enabled.

Format	**`no ip pimsm`**
Mode	Global Config

ip pimsm mode

This command sets administrative mode of PIM-SM multicast routing on a routing interface to enabled.

Default	disabled
Format	**`ip pimsm mode`**
Mode	Interface Config

no ip pimsm mode

This command sets administrative mode of PIM-SM multicast routing on a routing interface to the default value.

Format	**`no ip pimsm mode`**
Mode	Interface Config

ip pimsm query-interval

This command configures the transmission frequency of hello messages in seconds between PIM enabled neighbors. This field has a range of 10 to 3600 seconds.

Default	30
Format	**`ip pimsm query-interval`** *`<10-3600>`*
Mode	Interface Config

no ip pimsm query-interval

This command resets the transmission frequency of hello messages between PIM enabled neighbors to the default value.

Format	**`no ip pimsm query-interval`**
Mode	Interface Config

ip pimsm spt-threshold

This command is used to configure the Threshold rate for the RP router to switch to the shortest path. The rate is specified in Kilobytes per second. The possible values are 0 to 2000.

Default	50
Format	**`ip pimsm spt-threshold`** *<0-2000>*
Mode	Global Config

no ip pimsm spt-threshold

This command is used to reset the Threshold rate for the RP router to switch to the shortest path to the default value.

Format	**`no ip pimsm spt-threshold`**
Mode	Global Config

ip pim-trapflags

This command enables the PIM trap mode for both Sparse Mode (SM) and Dense Mode. (DM).

Default	disabled
Format	*`ip pim-trapflags`*
Mode	Global Config

no ip pim-trapflags

This command sets the PIM trap mode to the default.

Format	*no ip pim-trapflags*
Mode	Global Config

ip pimsm staticrp

This command is used to create RP IP address for the PIM-SM router. The parameter <*ipaddress*> is the IP address of the RP. The parameter <*groupaddress*> is the group address supported by the RP. The parameter <*groupmask*> is the group mask for the group address.

Default	disabled
Format	**ip pimsm staticrp** *<ipaddress> <groupaddress> <groupmask>*
Mode	Global Config

no ip pimsm staticrp

This command is used to delete RP IP address for the PIM-SM router. The parameter <*ipaddress*> is the IP address of the RP. The parameter <*groupaddress*> is the group address supported by the RP. The parameter <*groupmask*> is the group mask for the group address.

Format	**no ip pimsm staticrp** *<ipaddress> <groupaddress> <groupmask>*
Mode	Global Config

show ip pimsm

This command displays the system-wide information for PIM-SM.

Format	**`show ip pimsm`**
Modes	Privileged EXEC User EXEC

TABLE 6-18 Entry Definitions for `show ip pimsm`

Entry	Definition
PIM-SM Admin Mode	This field indicates whether PIM-SM is enabled or disabled.
Join/Prune Interval (secs)	The interval at which periodic PIM-SM Join/Prune messages are to be sent.
Data Threshold Rate (Kbps)	The data threshold rate for the PIM-SM router.
Register Threshold Rate (Kbps)	The threshold rate for the RP router to switch to the shortest path.
Interface	Valid slot and port number separated by forward slashes.
Interface Mode	This field indicates whether PIM-SM is enabled or disabled on the interface.
Protocol State	The current state of the PIM-SM protocol on the interface. Possible values are Operational or Non-Operational.

show ip pimsm candrptable

This command displays the IP multicast groups for which the local router is to advertise itself as a Candidate-RP when the value of hold time is non-zero.

Format	**`show ip pimsm candrptable`**
Modes	Privileged EXEC User EXEC

TABLE 6-19 Entry Definitions for `show ip pimsm candrptable`

Entry	Definition
Group Address	The IP multicast group address.
Group Mask	The multicast group address subnet mask.
Address	The unicast address of the interface that will be advertised as a Candidate-RP.

show ip pimsm componenttable

This command displays the table containing objects specific to a PIM domain. One row exists for each domain to which the router is connected.

Format	**`show ip pimsm componenttable`**
Modes	Privileged EXEC User EXEC

TABLE 6-20 Entry Definitions for `show ip pimsm componenttable`

Entry	Definition
Component Index	A number which uniquely identifies the component.
Component BSR Address	The IP address of the bootstrap router (BSR) for the local PIM region.
Component BSR Expiry Time	The minimum time remaining before the BSR in the local domain will be declared down.
Component CRP Hold Time	The hold time of the component when it is a candidate.

show ip pimsm interface

This command displays the interface information for PIM-SM on the specified interface.

Format	**`show ip pimsm interface`** *`<slot/port>`*
Modes	Privileged EXEC User EXEC

TABLE 6-21 Entry Definitions for `show ip pimsm interface`

Entry	Definition
Interface	Valid slot and port number separated by forward slashes.
IP Address	The IP address of the specified interface.
Subnet Mask	The Subnet Mask for the IP address of the PIM interface.
Mode	This field indicates whether PIM-SM is enabled or disabled on the specified interface. By default it is disabled.
Hello Interval	The frequency at which PIM hello messages are transmitted on this interface. By default, the value is 30 seconds.
CBSR Preference	The preference value for the local interface as a candidate bootstrap router.
CRP Preference	The preference value as a candidate rendezvous point on this interface.
CBSR Hash Mask Length	The hash mask length to be advertised in bootstrap messages if this interface is elected as the bootstrap router. The value is used in the hash algorithm for selecting the RP for a particular group.

show ip pimsm interface stats

This command displays the statistical information for PIM-SM on the specified interface.

Format	**`show ip pimsm interface stats`** *`{<slot/port> | all}`*
Modes	Privileged EXEC User EXEC

TABLE 6-22 Entry Definitions for `show ip pimsm interface` stats

Entry	Definition
Interface	Valid slot and port number separated by forward slashes.
IP Address	The IP Address that represents the PIM-SM interface.
Subnet Mask	The Subnet Mask of this PIM-SM interface.
Designated Router	The IP Address of the Designated Router for this interface.
Neighbor Count	The number of neighbors on the PIM-SM interface.

show ip pimsm neighbor

This command displays the neighbor information for PIM-SM on the specified interface.

Format	**`show ip pimsm neighbor`** *`{<slot/port>	all}`*
Modes	Privileged EXEC User EXEC

TABLE 6-23 Entry Definitions for `show ip pimsm neighbor`

Entry	Definition
Interface	Valid slot and port number separated by forward slashes.
IP Address	The IP Address of the neighbor on an interface.
Up Time	The time since this neighbor has become active on this interface.
Expiry Time	The expiry time of the neighbor on this interface.

show ip pimsm rp

This command displays the PIM information for candidate Rendezvous Points (RPs) for all IP multicast groups or for the specific <*groupaddress*> <*groupmask*> provided in the command. The information in the table is displayed for each IP multicast group.

Format	**`show ip pimsm rp`** *`{<groupaddress> <groupmask>	candidate	all}`*
Modes	Privileged EXEC User EXEC

TABLE 6-24 Entry Definitions for `show ip pimsm rp`

Entry	Definition
Group Address	The IP multicast group address.
Group Mask	The multicast group address subnet mask.
Address	The IP address of the Candidate-RP.

TABLE 6-24 Entry Definitions for `show ip pimsm rp`

Entry	Definition
Hold Time	The hold time of a Candidate-RP.
Expiry Time	The minimum time remaining before the Candidate-RP is declared down.
Component	A number which uniquely identifies the component. Each protocol instance connected to a separate domain should have a different index value.

show ip pimsm rphash

This command displays the RP router that will be selected from the set of active RP routers. The RP router, for the group, is selected by using the hash algorithm defined in RFC 2362.

Format	**`show ip pimsm rphash`** <*groupaddress*>
Modes	Privileged EXEC User EXEC
RP IP Address	The IP address of the RP.
Group Mask	The group mask for the group address.

show ip pimsm staticrp

This command displays the static RP information for the PIM-SM router.

Format	**`show ip pimsm staticrp`**
Modes	Privileged EXEC User EXEC
RP IP Address	The IP address of the RP.
Group Address	The group address supported by the RP.
Group Mask	The group mask for the group address.

Internet Group Message Protocol (IGMP) Commands

This section describes the commands you use to view and configure IGMP settings.

ip igmp

This command sets the administrative mode of IGMP in the system to active.

Default	disabled
Format	**`ip igmp`**
Mode	Global Config

no ip igmp

This command sets the administrative mode of IGMP in the system to inactive.

Format	**`no ip igmp`**
Mode	Global Config

ip igmp version

This command configures the version of IGMP for an interface. The value for *<version>* is either 1, 2 or 3.

Default	3
Format	**`ip igmp version`** **<***version***>**
Mode	Interface Config

`no ip igmp version`

This command resets the version of IGMP to the default value.

Format	**`no ip igmp version`**
Mode	Interface Config

`ip igmp last-member-query-count`

This command sets the number of Group-Specific Queries sent before the router assumes that there are no local members on the interface. The range for *<count>* is 1 to 20.

Format	**`ip igmp last-member-query-count`** *<count>*
Mode	Interface Config

`no ip igmp last-member-query-count`

This command resets the number of Group-Specific Queries to the default value.

Format	**`no ip igmp last-member-query-count`**
Mode	Interface Config

`ip igmp last-member-query-interval`

This command configures the Maximum Response Time inserted in Group-Specific Queries which are sent in response to Leave Group messages. The range for *<seconds>* is 0 to 255 tenths of a second.

Default	10 tenths of a second (1 second)
Format	**`ip igmp last-member-query-interval <`***seconds***`>`**
Mode	Interface Config

no ip igmp last-member-query-interval

This command resets the Maximum Response Time to the default value.

Format	**`no ip igmp last-member-query-interval`**
Mode	Interface Config

ip igmp query-interval

This command configures the query interval for the specified interface. The query interval determines how fast IGMP Host-Query packets are transmitted on this interface. The range for `<queryinterval>` is 1 to 3600 seconds.

Default	125 seconds
Format	**`ip igmp query-interval <`***`seconds`***`>`**
Mode	Interface Config

no ip igmp query-interval

This command resets the query interval for the specified interface to the default value. This is the frequency at which IGMP Host-Query packets are transmitted on this interface.

Format	**`no ip igmp query-interval`**
Mode	Interface Config

ip igmp query-max-response-time

This command configures the maximum response time interval for the specified interface, which is the maximum query response time advertised in IGMPv2 queries on this interface.The time interval is specified in tenths of a second. The range for *<maxresptime>* is 0 to 255 tenths of a second.

Default	100
Format	**ip igmp query-max-response-time <*seconds*>**
Mode	Interface Config

no ip igmp query-max-response-time

This command resets the maximum response time interval for the specified interface, which is the maximum query response time advertised in IGMPv2 queries on this interface to the default value. The maximum response time interval is reset to the default time.

Format	**no ip igmp query-max-response-time**
Mode	Interface Config

ip igmp robustness

This command configures the robustness that allows tuning of the interface. The robustness is the tuning for the expected packet loss on a subnet. If a subnet is expected to have a lot of loss, the Robustness variable may be increased for the interface. The range for *<robustness>* is 1 to 255.

Default	2
Format	**ip igmp robustness <*robustness*>**
Mode	Interface Config

no ip igmp robustness

This command sets the robustness value to default.

Format	**`no ip igmp robustness`**
Mode	Interface Config

ip igmp startup-query-count

This command sets the number of Queries sent out on startup, separated by the Startup Query Interval on the interface. The range for *<count>* is 1 to 20.

Default	2
Format	**`ip igmp startup-query-count <`***`count`***`>`**
Mode	Interface Config

no ip igmp startup-query-count

This command resets the number of Queries sent out on startup, separated by the Startup Query Interval on the interface to the default value.

Format	**`no ip igmp startup-query-count`**
Mode	Interface Config

ip igmp startup-query-interval

This command sets the interval between General Queries sent on startup on the interface. The time interval value is in seconds. The range for *<interval>* is 1 to 300 seconds.

Default	31
Format	**`ip igmp startup-query-interval <`***`interval`***`>`**
Mode	Interface Config

`no ip igmp startup-query-interval`

This command resets the interval between General Queries sent on startup on the interface to the default value.

Format	**`no ip igmp startup-query-interval`**
Mode	Interface Config

`show ip igmp`

This command displays the system-wide IGMP information.

Format	**`show ip igmp`**
Modes	Privileged EXEC User EXEC

TABLE 6-25 Entry Definitions for `show ip igmp`

Entry	**Definition**
IGMP Admin Mode	This field displays the administrative status of IGMP. This is a configured value.
Interface	Valid slot and port number separated by forward slashes.
Interface Mode	This field indicates whether IGMP is enabled or disabled on the interface. This is a configured value.
Protocol State	This field indicates the current state of IGMP on this interface. Possible values are Operational or Non-Operational.

`show ip igmp groups`

This command displays the registered multicast groups on the interface. If *`[detail]`* is specified this command displays the registered multicast groups on the interface in detail.

Format	**`show ip igmp groups`** ***`<slot/port> [detail]`***
Mode	**Privileged EXEC**

TABLE 6-26 Entry Definitions for `show ip igmp groups`

Entry	Definition
IP Address	This displays the IP address of the interface participating in the multicast group.
Subnet Mask	This displays the subnet mask of the interface participating in the multicast group.
Interface Mode	This displays whether IGMP is enabled or disabled on this interface.
	The following fields are not displayed if the interface is not enabled:
Querier Status	This displays whether the interface has IGMP in Querier mode or Non-Querier mode.
Groups	This displays the list of multicast groups that are registered on this interface.
	If you use the **`detail`** keyword, the following fields appear:
Multicast IP Address	This displays the IP Address of the registered multicast group on this interface.
Last Reporter	This displays the IP Address of the source of the last membership report received for the specified multicast group address on this interface.
Up Time	This displays the time elapsed since the entry was created for the specified multicast group address on this interface.
Expiry Time	This displays the amount of time remaining to remove this entry before it is aged out.
Version1 Host Timer	This displays the time remaining until the local router assumes that there are no longer any IGMP version 1 multicast members on the IP subnet attached to this interface. This could be an integer value or "-----" if there is no Version 1 host present.
Version2 Host Timer	This displays the time remaining until the local router assumes that there are no longer any IGMP version 2 multicast members on the IP subnet attached to this interface. This could be an integer value or "-----" if there is no Version 2 host present.
Group Compatibility Mode	The group compatibility mode (v1, v2 or v3) for this group on the specified interface.

`show ip igmp interface`

This command displays the IGMP information for the interface.

Format	**`show ip igmp interface`** `<`*`slot/port`*`>`
Modes	Privileged EXEC User EXEC

TABLE 6-27 Entry Definitions for `show ip igmp interface`

Entry	Definition
Interface	Valid slot and port number separated by forward slashes.
IGMP Admin Mode	The administrative status of IGMP.
Interface Mode	This field indicates whether IGMP is enabled or disabled on the interface.
IGMP Version	The version of IGMP running on the interface. This value can be configured to create a router capable of running either IGMP version 1 or 2.
Query Interval	The frequency at which IGMP Host-Query packets are transmitted on this interface.
Query Max Response Time	The maximum query response time advertised in IGMPv2 queries on this interface.
Robustness	The tuning for the expected packet loss on a subnet. If a subnet is expected to be have a lot of loss, the Robustness variable may be increased for that interface.
Startup Query Interval	The interval between General Queries sent by a Querier on startup.
Startup Query Count	The number of Queries sent out on startup, separated by the Startup Query Interval.
Last Member Query Interval	The Maximum Response Time inserted into Group-Specific Queries sent in response to Leave Group messages.
Last Member Query Count	The number of Group-Specific Queries sent before the router assumes that there are no local members.

show ip igmp interface membership

This command displays the list of interfaces that have registered in the multicast group.

Format	**`show ip igmp interface membership`** *`<multiipaddr>`* *`[detail]`*
Mode	Privileged EXEC

TABLE 6-28 Entry Definitions for `show ip igmp interface membership`

Entry	Definition
Interface	Valid unit, slot and port number separated by forward slashes.
Interface IP	The IP address of the interface participating in the multicast group.
State	The interface that has IGMP in Querier mode or Non-Querier mode.
Group Compatibility Mode	The group compatibility mode (v1, v2 or v3) for the specified group on this interface.
Source Filter Mode	The source filter mode (Include/Exclude) for the specified group on this interface. This is "-----" for IGMPv1 and IGMPv2 Membership Reports. If you use the **`detail`** keyword, the following fields appear:
Interface	Valid unit, slot and port number separated by forward slashes.
Group Compatibility Mode	The group compatibility mode (v1, v2 or v3) for the specified group on this interface.
Source Filter Mode	The source filter mode (Include/Exclude) for the specified group on this interface. This is "-----" for IGMPv1 and IGMPv2 Membership Reports.
Source Hosts	The list of unicast source IP Addresses in the group record of the IGMPv3 Membership Report with the specified multicast group IP Address. This is "-----" for IGMPv1 and IGMPv2 Membership Reports.
Expiry Time	The amount of time remaining to remove this entry before it is aged out. This is "-----" for IGMPv1 and IGMPv2 Membership Reports.

`show ip igmp interface stats`

This command displays the IGMP statistical information for the interface. The statistics are only displayed when the interface is enabled for IGMP.

Format	**`show ip igmp interface stats`** *`<slot/port>`*
Modes	Privileged EXEC User EXEC

TABLE 6-29 Entry Definitions for `show ip igmp interface stats`

Entry	Definition
Querier Status	The status of the IGMP router, whether it is running in Querier mode or Non-Querier mode.
Querier IP Address	The IP Address of the IGMP Querier on the IP subnet to which this interface is attached.
Querier Up Time	The time since the interface Querier was last changed.
Querier Expiry Time	The amount of time remaining before the Other Querier Present Timer expires. If the local system is the querier, the value of this object is zero.
Wrong Version Queries	The number of queries received whose IGMP version does not match the IGMP version of the interface.
Number of Joins	The number of times a group membership has been added on this interface.
Number of Groups	The current number of membership entries for this interface

IGMP Proxy Commands

The IGMP Proxy is used by IGMP Router (IPv4 system) to enable the system to issue IGMP host messages on behalf of hosts that the system discovered through standard IGMP router interfaces. With IGMP Proxy enabled, the system acts as proxy to all the hosts residing on its router interfaces.

ip igmp-proxy

This command enables the IGMP Proxy on the router. To enable the IGMP Proxy on the router, you must enable multicast forwarding. Also, make sure that there are no multicast routing protocols enabled on the router.

Format	**`ip igmp-proxy`**
Mode	Interface Config

no ip igmp-proxy

This command disables the IGMP Proxy on the router.

Format	**`no ip igmp-proxy`**
Mode	Interface Config

ip igmp-proxy unsolicit-rprt-interval

This command sets the unsolicited report interval for the IGMP Proxy router. This command is valid only when you enable IGMP Proxy on the interface. The value of *<interval>* can be 1-260 seconds.

Default	1
Format	**`ip igmp-proxy unsolicit-rprt-interval`** *<interval>*
Mode	Interface Config

no ip igmp-proxy unsolicit-rprt-interval

This command resets the unsolicited report interval of the IGMP Proxy router to the default value.

Format	**`no ip igmp-proxy unsolicit-rprt-interval`**
Mode	Interface Config

ip igmp-proxy reset-status

This command resets the host interface status parameters of the IGMP Proxy router. This command is valid only when you enable IGMP Proxy on the interface.

Format	**`ip igmp-proxy reset-status`**
Mode	Interface Config

show ip igmp-proxy

This command displays a summary of the host interface status parameters. It displays the following parameters only when you enable IGMP Proxy.

Format	**`show ip igmp-proxy`**
Mode	Privileged EXEC User EXEC

TABLE 6-30 Entry Definitions for `show ip igmp-proxy`

Entry	**Definition**
Interface index	The interface number of the IGMP Proxy.
Admin Mode	States whether the IGMP Proxy is enabled or not. This is a configured value.
Operational Mode	States whether the IGMP Proxy is operationally enabled or not. This is a status parameter.
Version	The present IGMP host version that is operational on the proxy interface.

TABLE 6-30 Entry Definitions for `show ip igmp-proxy`

Entry	Definition
Number of Multicast Groups	States the number of multicast groups that are associated with the IGMP Proxy interface.
Unsolicited Report Interval	The time interval at which the IGMP Proxy interface sends unsolicited group membership report.
Querier IP Address on Proxy Interface	The IP address of the Querier, if any, in the network attached to the upstream interface (IGMP-Proxy interface).
Older Version 1 Querier Timeout	The interval used to timeout the older version 1 queriers.
Older Version 2 Querier Timeout	The interval used to timeout the older version 2 queriers.
Proxy Start Frequency	The number of times the IGMP Proxy has been stopped and started.

show ip igmp-proxy interface

This command displays a detailed list of the host interface status parameters. It displays the following parameters only when you enable IGMP Proxy.

Format	**`show ip igmp-proxy interface`**
Mode	Privileged EXEC User EXEC

TABLE 6-31 Entry Definitions for `show ip igmp-proxy interface`

Entry	Definition
Interface Index	Shows the slot/port of the IGMP proxy. The column headings of the table associated with the interface are as follows:
Ver	Shows the IGMP version.
Query Rcvd	Number of IGMP queries received.
Report Rcvd	Number of IGMP reports received.
Report Sent	Number of IGMP reports sent.
Leaves Rcvd	Number of IGMP leaves received.
Leaves Sent	Number of IGMP leaves sent.

show ip igmp-proxy groups

This command displays information about the subscribed multicast groups that IGMP Proxy reported. It displays a table of entries with the following as the fields of each column.

Format	**`show ip igmp-proxy groups`**
Mode	Privileged EXEC User EXEC

TABLE 6-32 Entry Definitions for `show ip igmp-proxy groups`

Entry	Definition
Interface	The interface number of the IGMP Proxy.
Group Address	The IP address of the multicast group.
Last Reporter	The IP address of host that last sent a membership report.
Up Time (in secs)	The time elapsed since last created.
Member State	The status of the entry. Possible values are IDLE_MEMBER or DELAY_MEMBER. • IDLE_MEMBER - interface has responded to the latest group membership query for this group. • DELAY_MEMBER - interface is going to send a group membership report to respond to a group membership query for this group.
Filter Mode	Possible values are Include or Exclude.
Sources	The number of sources attached to the multicast group.

show ip igmp-proxy groups detail

This command displays complete information about multicast groups that IGMP Proxy reported. It displays a table of entries with the following as the fields of each column.

Format	**`show ip igmp-proxy groups detail`**
Mode	Privileged EXEC User EXEC

TABLE 6-33 Entry Definitions for `show ip igmp-proxy groups detail`

Entry	Definition
Interface	The interface number of the IGMP Proxy.
Group Address	The IP address of the multicast group.
Last Reporter	The IP address of host that last sent a membership report for the current group, on the network attached to the IGMP-Proxy interface (upstream interface).
Up Time (in secs)	The time elapsed since last created.
Member State	The status of the entry. Possible values are IDLE_MEMBER or DELAY_MEMBER. • IDLE_MEMBER - interface has responded to the latest group membership query for this group. • DELAY_MEMBER - interface is going to send a group membership report to respond to a group membership query for this group.
Filter Mode	Possible values are include or exclude.
Sources	The number of sources attached to the multicast group.
Group Source List	The list of IP addresses of the sources attached to the multicast group.
Expiry Time	Time left before a source is deleted.

CHAPTER 7

Quality of Service (QoS) Commands

This chapter describes the Quality of Service (QoS) commands available in the FASTPATH® CLI.

The commands in this chapter are in two functional groups:

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

This chapter contains the following sections:

Class of Service (CoS) Commands

This section describes the commands you use to configure and view Class of Service (CoS) settings for the switch. The commands in this section allow you to control the priority and transmission rate of traffic.

Note – Commands you issue in the Interface Config mode only affect a single interface. Commands you issue in the Global Config mode affect all interfaces.

`classofservice dot1p-mapping`

This command maps an 802.1p priority to an internal traffic class. The *`<userpriority>`* values can range from 0-7. The *`<trafficclass>`* values range from 0-6, although the actual number of available traffic classes depends on the platform. For more information about 802.1p priority, see "Provisioning (IEEE 802.1p) Commands" on page 74.

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-precedence-mapping

This command maps an IP precedence value to an internal traffic class. The *<ip-precedence>* values can range from 0-7. The *<trafficclass>* values can range from 0-6, although the actual number of available traffic classes depends on the platform.

Format	**`classofservice ip-precedence-mapping`** *`<ip-precedence> <trafficclass>`*
Modes	Global Config Interface Config

no classofservice ip-precedence-mapping

This command maps each IP precedence value to its default internal traffic class value.

Format	**`no classofservice ip-precedence-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 trust

This command sets the class of service trust mode of an interface. 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	ip-precedence	untrusted}`*
Mode	Global Config Interface Config

no classofservice trust

This command sets the interface mode to the default value.

Format	**`no classofservice trust`**
Modes	Global Config Interface Config

cos-queue min-bandwidth

This command specifies the minimum transmission bandwidth guarantee for each interface queue. 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 strict

This command activates the strict priority scheduler mode for each specified queue.

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

traffic-shape

This command specifies the maximum transmission bandwidth limit for the interface as a whole. Also known as rate shaping, traffic shaping has the effect of smoothing temporary traffic bursts over time so that the transmitted traffic rate is bounded.

Format	**`traffic-shape`** *`<bw>`*
Modes	Global Config Interface Config

no traffic-shape

This command restores the interface shaping rate to the default value.

Format	**`no traffic-shape`**
Modes	Global Config
Interface Config	

show classofservice dot1p-mapping

This command displays the current Dot1p (802.1p) priority mapping to internal traffic classes for a specific interface. The `<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 "Provisioning (IEEE 802.1p) Commands" on page 74.

Format	**`show classofservice dot1p-mapping`** *`[<slot/port>]`*
Mode	Privileged EXEC

The following information is repeated for each user priority.

TABLE 7-1 Entry Definitions for User Priority

Entry	Definition
User Priority	The 802.1p user priority value.
Traffic Class	The traffic class internal queue identifier to which the user priority value is mapped.

show classofservice ip-precedence-mapping

This command displays the current IP Precedence mapping to internal traffic classes for a specific interface. The 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`** *`[<slot/port>]`*
Mode	Privileged EXEC

The following information is repeated for each user priority.

TABLE 7-2 Entry Definitions for IP Precedence

Entry	Definition
IP Precedence	The IP Precedence value
Traffic Class	The traffic class internal queue identifier to which the IP Precedence 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.

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

show classofservice trust

This command displays the current trust mode setting for a specific interface. The *<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`** *[<slot/port>]*
Mode	Privileged EXEC

TABLE 7-3 Entry Definitions for `show classofservice trust`

Entry	Definition
Non-IP Traffic Class	The traffic class used for non-IP traffic. This is only displayed when the COS trust mode is set to trust IP Precedence or IP DSCP (on platforms that support IP DSCP).
Untrusted Traffic Class	The traffic class used for all untrusted traffic. This is only displayed when the COS trust mode is set to 'untrusted'.

show interfaces cos-queue

This command displays the class-of-service queue configuration for the specified interface. The 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`** *`[<slot/port>]`*
Mode	Privileged EXEC

TABLE 7-4 Entry Definitions for `show interfaces cos-queue`

Entry	Definition
Queue Id	An interface supports n queues numbered 0 to (n-1). The specific n value is platform dependent.
Minimum Bandwidth	The minimum transmission bandwidth guarantee for the queue, expressed as a percentage. A value of 0 means bandwidth is not guaranteed and the queue operates using best-effort. This is a configured value.
Scheduler Type	Indicates whether this queue is scheduled for transmission using a strict priority or a weighted scheme. This is a configured value.
Queue Management Type	The queue depth management technique used for this queue (tail drop). If you specify the interface, the command also displays the following information.
Interface	This displays the slot/port of the interface. If displaying the global configuration, this output line is replaced with a Global Config indication.
Interface Shaping Rate	The maximum transmission bandwidth limit for the interface as a whole. It is independent of any per-queue maximum bandwidth value(s) in effect for the interface. This is a configured value.

Differentiated Services (DiffServ) Commands

This section describes the commands you use to configure QOS Differentiated Services (DiffServ).

You configure DiffServ in several stages by specifying three DiffServ components:

- Class:
  - Creating and deleting classes.
  - Defining match criteria for a class.
- Policy:
  - Creating and deleting policies
  - Associating classes with a policy
  - Defining policy statements for a policy/class combination
- Service: Adding and removing a policy to/from an inbound interface

The DiffServ class defines the packet filtering criteria. The attributes of a DiffServ policy define the way the switch processes packets. You can define policy attributes on a per-class instance basis. The switch applies these attributes when a match occurs.

Packet processing begins when the switch tests the match criteria for a packet. The switch applies a policy to a packet when it finds a class match within that policy.

The following rules apply when you create a DiffServ class:

- Each class can contain a maximum of one referenced (nested) class
- Class definitions do not support hierarchical service policies

A given class definition can contain a maximum of one reference to another class. You can combine the reference with other match criteria. The referenced class is truly a reference and not a copy since additions to a referenced class affect all classes that reference it. Changes to any class definition currently referenced by any other class must result in valid class definitions for all derived classes, otherwise the switch rejects the change. You can remove a class reference from a class definition.

The only way to remove an individual match criterion from an existing class definition is to delete the class and re-create it.

Note – The mark possibilities for policing include CoS, IP DSCP, and IP Precedence. While the latter two are only meaningful for IP packet types, CoS marking is allowed for both IP and non-IP packets, since it updates the 802.1p user priority field contained in the VLAN tag of the layer 2 packet header.

Note – Traffic to be processed by the DiffServ feature requires an IP 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.

Note – The CLI mode is changed to Class-Map Config when this command is successfully executed.

Format	**`class-map match-all`** *`<class-map-name>`*
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 (The *<class-map-name>* 'default' is reserved and must not be used here).

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.

Note – This command is not available on the Broadcom 5630x platform.

Format	**`match ethertype`** *`{<keyword>	custom <0x0600-0xFFFF>}`*
Mode	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.

Default	none
Format	**`match any`**
Mode	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.

- 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.

Default	none
Format	**`match class-map`** *`<refclassname>`*
Mode	Class-Map Config

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

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.

Note – This command is not available on the Broadcom 5630x platform.

Default	none
Format	**`match cos`** *<0-7>*
Mode	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.

Note – This command is not available on the Broadcom 5630x platform.

Default	none
Format	**`match secondary-cos`** *<0-7>*
Mode	Class-Map Config

match destination-address mac

This command adds to the specified class definition a match condition based on the destination MAC address of a packet. The <macaddr> parameter is any layer 2 MAC address formatted as six, two-digit hexadecimal numbers separated by colons (e.g., 00:11:22:dd:ee:ff). The <macmask> parameter is a layer 2 MAC address bit mask, which need not be contiguous, and is formatted as six, two-digit hexadecimal numbers separated by colons (e.g., ff:07:23:ff:fe:dc).

Note – This command is not available on the Broadcom 5630x platform.

Default	none
Format	**`match destination-address mac`** *`<macaddr> <macmask>`*
Mode	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.

Default	none
Format	**`match dstip`** *`<ipaddr> <ipmask>`*
Mode	Class-Map Config

match dstl4port

This command adds to the specified class definition a match condition based on the destination layer 4 port of a packet using a single keyword or numeric notation. To specify the match condition as a single keyword, the value for *`<portkey>`* is one of the supported port name keywords. The currently supported *`<portkey>`* values are: domain, echo, ftp, ftpdata, http, smtp, snmp, telnet, tftp, www. Each of these translates into its equivalent port number. To specify the match condition using a numeric notation, one layer 4 port number is required. The port number is an integer from 0 to 65535.

Default	none
Format	**`match dstl4port`** *`{<portkey>	<0-65535>}`*
Mode	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.

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 ip dscp`** *`<dscpval>`*
Mode	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.

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 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).

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 ip tos`** *`<tosbits> <tosmask>`*
Mode	Class-Map Config

match protocol

This command adds to the specified class definition a match condition based on the value of the IP Protocol field in a packet using a single keyword notation or a numeric value notation.

To specify the match condition using a single keyword notation, the value for <protocol-name> is one of the supported protocol name keywords. The currently supported values are: *`icmp`*, *`igmp`*, *`ip`*, *`tcp`*, *`udp`*. A value of *`ip`* matches all protocol number values.

To specify the match condition using a numeric value notation, the protocol number is a standard value assigned by IANA and is interpreted as an integer from 0 to 255.

Note – This command does not validate the protocol number value against the current list defined by IANA.

Default	none
Format	**`match protocol`** *`{<protocol-name> | <0-255>}`*
Mode	Class-Map Config

match source-address mac

This command adds to the specified class definition a match condition based on the source MAC address of a packet. The <address> parameter is any layer 2 MAC address formatted as six, two-digit hexadecimal numbers separated by colons (e.g., 00:11:22:dd:ee:ff). The <macmask> parameter is a layer 2 MAC address bit mask, which may not be contiguous, and is formatted as six, two-digit hexadecimal numbers separated by colons (e.g., ff:07:23:ff:fe:dc).

Note – This command is not available on the Broadcom 5630x platform.

Default	none
Format	**`match source-address mac`** *`<address> <macmask>`*
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.

Default	none
Format	**match srcip** *<ipaddr> <ipmask>*
Mode	Class-Map Config

match srcl4port

This command adds to the specified class definition a match condition based on the source layer 4 port of a packet using a single keyword or numeric notation. To specify the match condition as a single keyword notation, the value for *<portkey>* is one of the supported port name keywords (listed below). The currently supported *<portkey>* values are: domain, echo, ftp, ftpdata, http, smtp, snmp, telnet, tftp, www. Each of these translates into its equivalent port number, which is used as both the start and end of a port range.

To specify the match condition as a numeric value, one layer 4 port number is required. The port number is an integer from 0 to 65535.

Default	none
Format	**match srcl4port** *{<portkey> | <0-65535>}*
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 1 to 4095.

Note – This command is not available on the Broadcom 5630x platform.

Default	none
Format	**`match vlan`** *<1-4095>*
Mode	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 1 to 4095.

Note – This command is not available on the Broadcom 5630x platform.

Default	none
Format	**`match secondary-vlan`** *<1-4095>*
Mode	Class-Map Config

DiffServ Policy Commands

Use the DiffServ policy commands to specify traffic conditioning actions, such as policing and marking, to apply to traffic classes

Use the policy commands to associate a traffic class that you define by using the class command set with one or more QoS policy attributes. Assign the class/policy association to an interface to form a service. Specify the policy name when you create the policy.

Each traffic class defines a particular treatment for packets that match the class definition. You can associate multiple traffic classes with a single policy. When a packet satisfies the conditions of more than one class, preference is based on the order in which you add the classes to the policy. The first class you add has the highest precedence.

This set of commands consists of policy creation/deletion, class addition/removal, and individual policy attributes.

Note – The only way to remove an individual policy attribute from a class instance within a policy is to remove the class instance and re-add it to the policy. The values associated with an existing policy attribute can be changed without removing the class instance.

The CLI command root is **`policy-map`**.

assign-queue

This command modifies the queue id to which the associated traffic stream is assigned. The queueid is an integer from 0 to n-1, where n is the number of egress queues supported by the device.

Format	**`assign-queue`** *<queueid>*
Mode	Policy-Class-Map Config
Incompatibilities	Drop

drop

This command specifies that all packets for the associated traffic stream are to be dropped at ingress.

Format	**`drop`**
Mode	Policy-Class-Map Config
Incompatibilities	Assign Queue, Mark (all forms), Mirror, Police, Redirect

mirror

This command specifies that all incoming packets for the associated traffic stream are copied to a specific egress interface (physical port or LAG).

Note – This command is not available on the Broadcom 5630x platform.

Format	**`mirror`** *`<slot/port>`*
Mode	Policy-Class-Map Config
Incompatibilities	Drop, Redirect

redirect

This command specifies that all incoming packets for the associated traffic stream are redirected to a specific egress interface (physical port or port-channel).

Note – This command is not available on the Broadcom 5630x platform.

Format	**`redirect`** *`<slot/port>`*
Mode	Policy-Class-Map Config
Incompatibilities	Drop, Mirror

conform-color

Use this command to enable color-aware traffic policing and define the conform-color class map. Used in conjunction with the police command where the fields for the conform level are specified. The <class-map-name> parameter is the name of an existing Diffserv class map.

Note – This command may only be used after specifying a police command for the policy-class instance.

Format	**`conform-color`** *`<class-map-name>`*
Mode	Policy-Class-Map Config

class

This command creates an instance of a class definition within the specified policy for the purpose of defining treatment of the traffic class through subsequent policy attribute statements. The *<classname>* is the name of an existing DiffServ class.

Note – This command causes the specified policy to create a reference to the class definition.

Note – The CLI mode is changed to Policy-Class-Map Config when this command is successfully executed.

Format	**`class`** *<classname>*
Mode	Policy-Map Config

no class

This command deletes the instance of a particular class and its defined treatment from the specified policy. *<classname>* is the names of an existing DiffServ class.

Note – This command removes the reference to the class definition for the specified policy.

Format	**`no class`** *<classname>*
Mode	Policy-Map Config

mark cos

This command marks all packets for the associated traffic stream with the specified class of service 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 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.

Format	**`mark ip-precedence`** *`<0-7>`*
Mode	Policy-Class-Map Config
Policy Type	In
Incompatibilities	Drop, Mark CoS, Mark IP DSCP, Police

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-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.

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-prec-transmit <0-7> | set-dscp-transmit <0-63> | set-cos-transmit <0-7> | transmit} [violate-action {drop | set-prec-transmit <0-7> | set-dscp-transmit <0-63> | set-cos-transmit <0-7> | transmit}]}*
Mode	Policy-Class-Map Config
Incompatibilities	Drop, Mark (all forms)

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.

Note – The CLI mode is changed to Policy-Map Config when this command is successfully executed.

Format	**`policy-map`** *`<policyname>`* **`in`**
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. 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`** *`<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. 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. There is no separate interface administrative 'mode' command for DiffServ.

Format	**`no service-policy in`** *<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.

TABLE 7-5 Entry Definitions for `show class-map`

Entry	**Definition**
Class Name	The name of this class. If you do not specify the Class Name, this command displays a list of all defined DiffServ classes. See next table for definitions.
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.
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	This field displays the values of the Match Criteria. :

TABLE 7-6 Entry Definitions for `show class-map` (All)

Entry	**Definition**
Class Name	The name of this class. (Note that the order in which classes are displayed is not necessarily the same order in which they were created.)
Class Type	A class type of 'all' means every match criterion defined for the class is evaluated simultaneously and must all be true to indicate a class match.
Ref Class Name	The name of an existing DiffServ class whose match conditions are being referenced by the specified class definition.

`show diffserv`

This command displays the DiffServ General Status Group information, which includes the current administrative mode setting as well as the current and maximum number of rows in each of the main DiffServ private MIB tables. This command takes no options.

Format	**`show diffserv`**
Mode	Privileged EXEC

TABLE 7-7 Entry Definitions for `show diffserv`

Entry	Definition
DiffServ Admin mode	The current value of the DiffServ administrative mode.
Class Table Size	The current number of entries (rows) in the Class Table.
Class Table Max	The maximum allowed entries (rows) for the Class Table.
Class Rule Table Size	The current number of entries (rows) in the Class Rule Table.
Class Rule Table Max	The maximum allowed entries (rows) for the Class Rule Table.
Policy Table Size	The current number of entries (rows) in the Policy Table.
Policy Table Max	The maximum allowed entries (rows) for the Policy Table.
Policy Instance Table Size	Current number of entries (rows) in the Policy Instance Table.
Policy Instance Table Max	Maximum allowed entries (rows) for the Policy Instance Table.
Policy Attribute Table Size	Current number of entries (rows) in the Policy Attribute Table.
Policy Attribute Table Max	Maximum allowed entries (rows) for the Policy Attribute Table.
Service Table Size	The current number of entries (rows) in the Service Table.
Service Table Max	The maximum allowed entries (rows) for the Service Table.

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.

TABLE 7-8

Entry	Definition
Policy Name	The name of this policy.
Type	The policy type (Only inbound policy definitions are supported for this platform.)

The following information is repeated for each class associated with this policy (only those policy attributes actually configured are displayed).

TABLE 7-9 Entry Definitions for `show policy-map`

Entry	Definition
Assign Queue	Directs traffic stream to the specified QoS queue. This allows a traffic classifier to specify which one of the supported hardware queues are used for handling packets belonging to the class.
Class Name	The name of this class.
Committed Burst Size (KB)	This field displays the committed burst size, used in simple policing.
Committed Rate (Kbps)	This field displays 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 COS	This field shows the CoS mark value if the conform action is set-cos-transmit.
Conform DSCP Value	This field shows the DSCP mark value if the conform action is set-dscp-transmit.
Conform IP Precedence Value	This field shows the IP Precedence mark value if the conform action is set-prec-transmit.
Drop	Drop a packet upon arrival. This is useful for emulating access control list operation using DiffServ, especially when DiffServ and ACL cannot co-exist on the same interface.
Mark CoS	Denotes 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 IP DSCP	Denotes 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.

TABLE 7-9 Entry Definitions for `show policy-map` *(Continued)*

Entry	Definition
Mark IP Precedence	Denotes the mark/re-mark value used as the IP Precedence for traffic matching this class. This is not displayed if mark ip precedence is not specified.
Mirror	Copies a classified traffic stream to a specified egress port (physical port or LAG). This can occur in addition to any marking or policing action. It may also be specified along with a QoS queue assignment. This field does not display on Broadcom 5630x platforms.
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	This field displays the CoS mark value if the non-conform action is set-cos-transmit.
Non-Conform DSCP Value	This field displays the DSCP mark value if the non-conform action is set-dscp-transmit.
Non-Conform IP Precedence Value	This field displays the IP Precedence mark value if the non-conform action is set-prec-transmit.
Policing Style	This field denotes the style of policing, if any, used (simple).
Redirect	Forces a classified traffic stream to a specified egress port (physical port or LAG). This can occur in addition to any marking or policing action. It may also be specified along with a QoS queue assignment. This field does not display on Broadcom 5630x platforms.

If the Policy Name is not specified this command displays a list of all defined DiffServ policies. The following fields are displayed.

TABLE 7-10 Entry Definitions for `show policy-map` Without Specifying Policy Name

Entry	Definition
Policy Name	The name of this policy. (The order in which the policies are displayed is not necessarily the same order in which they were created.)
Policy Type	The policy type (Only inbound is supported).
Class Members	List of all class names associated with this policy.

`show diffserv service`

This command displays policy service information for the specified interface and direction. The *`<slot/port>`* parameter specifies a valid slot/port number for the system.

Format	**`show diffserv service`** *`<slot/port>`* **`in`**
Mode	Privileged EXEC

TABLE 7-11 Entry Definitions for `show diffserv service`

Entry	Definition
DiffServ Admin Mode	The current setting of the DiffServ administrative mode. An attached policy is only in effect on an interface while DiffServ is in an enabled mode.
Interface	Valid slot and port number separated by forward slashes.
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

TABLE 7-12 Entry Definitions for `show diffserv service brief`

Entry	Definition
DiffServ Mode	The current setting of the DiffServ administrative mode. An attached policy is only active on an interface while DiffServ is in an enabled mode. The following information is repeated for interface and direction (only those interfaces configured with an attached policy are shown):.
Interface	Valid slot and port number separated by forward slashes.
Direction	The traffic direction of this interface service.
OperStatus	The current operational status of this DiffServ service interface.
Policy Name	The name of the policy attached to the interface in the indicated direction.

`show policy-map interface`

This command displays policy-oriented statistics information for the specified interface and direction. The *<slot/port>* parameter specifies a valid interface for the system.

Note – This command is only allowed while the DiffServ administrative mode is enabled.

Format	**`show policy-map interface`** *`<slot/port> [in]`*
Mode	Privileged EXEC

TABLE 7-13 Entry Definitions for `show policy-map interface`

Entry	Definition
Interface	Valid slot and port number separated by forward slashes.
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.
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).

TABLE 7-14 Entry Definitions for `show service-policy`

Entry	Definition
Interface	Valid slot and port number separated by forward slashes.
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 (ACL) Commands

This section describes the commands you use 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 create is 100, regardless of type.
- The system supports only Ethernet II frame types.
- The maximum number of rules per MAC ACL is hardware dependent.
- For the Broadcom 5630x platform, if you configure an IP ACL on an interface, you cannot configure a MAC ACL on the same interface.

`mac access-list extended`

This command creates a MAC Access Control List (ACL) identified by *<name>*, consisting of classification fields defined for the Layer 2 header of an Ethernet frame. The *<name>* parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the MAC access list.

If a MAC ACL by this name already exists, this command enters Mac-Access-List config mode to allow updating the existing MAC ACL.

Note – The CLI mode changes to Mac-Access-List Config mode when you successfully execute this command.

Format	**`mac access-list extended`** *<name>*
Mode	Global Config

`no mac access-list extended`

This command deletes a MAC ACL identified by *<name>* from the system.

Format	**`no mac access-list extended`** *<name>*
Mode	Global Config

`mac access-list extended rename`

This command changes the name of a MAC Access Control List (ACL). The *<name>* parameter is the name of an existing MAC ACL. The *<newname>* parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the MAC access list.

This command fails if a MAC ACL by the name *<newname>* already exists.

Format	**`mac access-list extended rename`** *<name> <newname>*
Mode	Global Config

`{deny | permit}`

This command creates a new rule for the current MAC access list. Each rule is appended to the list of configured rules for the list.

Note – The 'no' form of this command is not supported, since the rules within a MAC ACL cannot be deleted individually. Rather, the entire MAC ACL must be deleted and re-specified.

Note – An implicit 'deny all' MAC rule always terminates the access list.

Note – For BCM5630x and BCM5650x based systems, assign-queue, redirect, and mirror attributes are configurable for a deny rule, but they have no operational effect.

A rule may either deny or permit traffic according to the specified classification fields. At a minimum, the source and destination MAC value must be specified, each of which may be substituted using the keyword any to indicate a match on any value in that field. The remaining command parameters are all optional, but the most frequently used parameters appear in the same relative order as shown in the command format.

The Ethertype may be specified as either a keyword or a four-digit hexadecimal value from 0x0600-0xFFFF. The currently supported *`<ethertypekey>`* values are: appletalk, arp, ibmsna, ipv4, ipv6, ipx, mplsmcast, mplsucast, netbios, novell, pppoe, rarp. Each of these translates into its equivalent Ethertype value(s).

TABLE 7-15 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

TABLE 7-15 Ethertype Keyword and 4-digit Hexadecimal Value *(Continued)*

Ethertype Keyword	Corresponding Value
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 assign-queue parameter allows specification of a particular hardware queue for handling traffic that matches this rule. The allowed <queue-id> value is 0-(n-1), where n is the number of user configurable queues available for the hardware platform. The *`assign-queue`* parameter is valid only for a **`permit`** rule.

For the Broadcom 5650x platform, the *`mirror`* parameter allows the traffic matching this rule to be copied to the specified *`<slot/port>`*, while the redirect parameter allows the traffic matching this rule to be forwarded to the specified *`<slot/port>`*. The *`assign-queue`* and *`redirect`* parameters are only valid for a **`permit`** rule.

Note – The *`mirror`* and *`redirect`* parameters are not available on the Broadcom 5630x platform.

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.

Format	*`{deny|permit} {<srcmac> | any} {<dstmac> | any} [<ethertypekey> | <0x0600-0xFFFF>] [vlan {eq <0-4095>}] [cos <0-7>] [[log] [assign-queue <queue-id>]] [{mirror | redirect} <slot/port>]`*
Mode	Mac-Access-List Config

`mac access-group`

This command attaches a specific MAC Access Control List (ACL) identified by *`<name>`* to an interface 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 'Interface Config' mode command is only available on platforms that support independent per-port class of service queue configuration.

Format	**`mac access-group`** *`<name>`* **`in`** *`[sequence <1-4294967295>]`*
Modes	Global Config Interface Config

`no mac access-group`

This command removes a MAC ACL identified by *`<name>`* from the interface in a given direction.

Format	**`no mac access-list`** *`<name>`* **`in`**
Modes	Global Config Interface Config

`show mac access-lists`

This command displays a MAC access list and all of the rules that are defined for the MAC ACL. Use the *`[name]`* parameter to identify a specific MAC ACL to display.

Format	**`show mac access-lists`** *`[name]`*
Mode	Privileged EXEC

TABLE 7-16 Entry Definitions for `show mac access-lists`

Entry	Definition
Rule Number	The ordered rule number identifier defined within the MAC ACL.
Action	Displays the action associated with each rule. The possible values are Permit or Deny.
Source MAC Address	Displays the source MAC address for this rule.
Destination MAC Address	Displays the destination MAC address for this rule.
Ethertype	Displays the Ethertype keyword or custom value for this rule.
VLAN ID	Displays the VLAN identifier value or range for this rule.
COS	Displays the COS (802.1p) value for this rule.
Log	Displays when you enable logging for the rule.
Assign Queue	Displays the queue identifier to which packets matching this rule are assigned.
Mirror Interface	On Broadcom 5650x platforms, displays the unit/slot/port to which packets matching this rule are copied.
Redirect Interface	On Broadcom 5650x platforms, displays the slot/port to which packets matching this rule are forwarded.

IP Access Control List (ACL) Commands

This section describes the commands you use 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:

- FASTPATH does not support IP ACL configuration for IP packet fragments.
- The maximum number of ACLs you can create is 100, regardless of type.
- The maximum number of rules per IP ACL is hardware dependent.
- On Broadcom 5630x platforms, if you configure a MAC ACL on an interface, you cannot configure an IP ACL on the same interface.
- Wildcard masking for ACLs operates differently from a subnet mask. A wildcard mask is in essence the inverse of a subnet mask. With a subnet mask, the mask has ones (1's) in the bit positions that are used for the network address, and has zeros (0's) for the bit positions that are not used. In contrast, a wildcard mask has (0's) in a bit position that must be checked. A '1' in a bit position of the ACL mask indicates the corresponding bit can be ignored.

access-list

This command creates an IP Access Control List (ACL) that is identified by the access list number, which is 1-99 for standard ACLs or 100-199 for extended ACLs. Table 7-17 describes the parameters for the **`access-list`** command.

IP Standard ACL:

Format	**`access-list`** *`<1-99> {deny	permit} {every	<srcip> <srcmask>} [log] [assign-queue <queue-id>] [{mirror	redirect} <unit/slot/port>]`*
Mode	Global Config

IP Extended ACL:

Format	**access-list** *<100-199> {deny | permit} {every | {{icmp | igmp | ip | tcp | udp | <number>} <srcip> <srcmask>[{eq {<portkey> | <0-65535>} <dstip> <dstmask> [{eq {<portkey>| <0-65535>}] [precedence <precedence> | tos <tos> <tosmask> | dscp <dscp>] [log] [assign-queue <queue-id>] [{mirror | redirect} <unit/slot/port>]*
Mode	Global Config

TABLE 7-17 ACL Command Parameters

Parameter	Description
<1-99> or <100-199>	Range 1 to 99 is the access list number for an IP standard ACL. Range 100 to 199 is the access list number for an IP extended ACL.
{deny | permit}	Specifies whether the IP ACL rule permits or denies an action. **Note -** For 5630x and 5650x-based systems, assign-queue, redirect, and mirror attributes are configurable for a deny rule, but they have no operational effect.
every	Match every packet
{icmp | igmp | ip | tcp | udp | <number>}	Specifies the protocol to filter for an extended IP ACL rule.
<srcip> <srcmask>	Specifies a source IP address and source netmask for match condition of the IP ACL rule.
[{eq {<portkey> | <0-65535>}]	Specifies the source layer 4 port match condition for the IP ACL rule. You can use the port number, which ranges from 0-65535, or you specify the *<portkey>*, which can be one of the following keywords: *domain, echo, ftp, ftpdata, http, smtp, snmp, telnet, tftp*, and *www*. Each of these keywords translates into its equivalent port number, which is used as both the start and end of a port range.
<dstip> <dstmask>	Specifies a destination IP address and netmask for match condition of the IP ACL rule.
[precedence <precedence> | tos <tos> <tosmask> | dscp <dscp>]	Specifies the TOS for an IP ACL rule depending on a match of precedence or DSCP values using the parameters *dscp, precedence*, *tos/tosmask*.
[log]	Specifies that this rule is to be logged.

TABLE 7-17 ACL Command Parameters

Parameter	Description
[assign-queue <queue-id>]	Specifies the assign-queue, which is the queue identifier to which packets matching this rule are assigned.
[{mirror | redirect} <slot/port>]	For Broadcom 5650x platforms, specifies the mirror or redirect interface which is the slot/port to which packets matching this rule are copied or forwarded, respectively. The `mirror` and `redirect` parameters are not available on the Broadcom 5630x platform.

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>*
Mode	Global Config

ip access-group

This command attaches a specified IP ACL to one interface or to all interfaces.

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.

Default	none
Format	**`ip access-group`** *<accesslistnumber>* **`in`** *[sequence <1-4294967295>]*
Modes	Interface Config Global Config

no ip access-group

This command removes a specified IP ACL from an interface.

Default	none
Format	**`no ip access-group`** *`<accesslistnumber>`* **`in`**
Mode	Interface Config

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

This command displays an IP ACL *`<accesslistnumber>`* is the number used to identify the IP ACL.

Format	**`show ip access-lists`** *`<accesslistnumber>`*
Mode	Privileged EXEC

Note – Only the access list fields that you configure are displayed.

TABLE 7-18 Entry Definitions for `show ip access-lists`

Entry	Definition
Rule Number	This displays the number identifier for each rule that is defined for the IP ACL.
Action	This displays the action associated with each rule. The possible values are Permit or Deny.
Match All	Indicates whether this access list applies to every packet. Possible values are True or False.
Protocol	This displays the protocol to filter for this rule.
Source IP Address	This displays the source IP address for this rule.
Source IP Mask	This field displays the source IP Mask for this rule.
Source L4 Port Keyword	This field displays the source port for this rule.
Destination IP Address	This displays the destination IP address for this rule.
Destination IP Mask	This field displays the destination IP Mask for this rule.
Destination L4 Port Keyword	This field displays the destination port for this rule.
IP DSCP	This field indicates the value specified for IP DSCP.
IP Precedence	This field indicates the value specified IP Precedence.
IP TOS	This field indicates the value specified for IP TOS.
Log	Displays when you enable logging for the rule.
Assign Queue	Displays the queue identifier to which packets matching this rule are assigned.
Mirror Interface	Displays the unit/slot/port to which packets matching this rule are copied.
Redirect Interface	Displays the unit/slot/port to which packets matching this rule are forwarded.

show access-lists

This command displays IP ACLs and MAC access control lists information for a designated interface and direction.

Format	**`show access-lists interface`** *`<slot/port>`* **`in`**
Mode	Privileged EXEC

TABLE 7-19 Entry Definitions for `show access-lists`

Entry	Definition
ACL Type	Type of access list (IP or MAC).
ACL ID	Access List name for a MAC 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).

CHAPTER 8

Utility Commands

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

The commands in this chapter are presented in four 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.

This chapter includes the following sections:

Dual Image Commands

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

delete

This command deletes the supplied image file from the permanent storage. The image to be deleted must be a backup image. If this image is the active image, or if this image is activated, error is displayed.

Format	**`delete`** *`{image1	image2}`*
Mode	Privileged EXEC

boot system

This command activates the specified image. It will be the active-image for subsequent reboots and will be to 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 error.

Format	**`boot system`** *`<image-file-name>`*
Mode	Privileged EXEC

show bootvar

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

Format	**`show bootvar`**
Mode	Privileged EXEC

`filedescr`

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

Format	**`filedescr`** *`{image1	image2} <text-description>`*
Mode	Privileged EXEC

`update bootcode`

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

Format	**`update bootcode`**
Mode	Privileged EXEC

System Information and Statistics Commands

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

`show arp switch`

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

Format	**`show arp switch`**
Mode	Privileged EXEC

TABLE 8-1

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

`show eventlog`

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

Format	**`show eventlog`**
Mode	Privileged EXEC

TABLE 8-2 Entry Definitions for `show eventlog`

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

Note – Event log information is retained across a switch reset.

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 "show version" command.

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

TABLE 8-3 Entry Definitions for `show version`

Entry	**Definition**
Switch Description	Text used to identify the product name of this switch.
Machine Type	Specifies the machine model as defined by the Vital Product Data.
Machine Model	Specifies 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	Indicates hardware changes that are significant to software.
Manufacturer	Manufacturer descriptor field.

TABLE 8-3 Entry Definitions for `show version` *(Continued)*

Entry	Definition
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	This displays the additional packages incorporated into this system.

`show interface`

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

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

The display parameters, when the argument is *`<slot/port>`*, is as follows.

TABLE 8-4 Entry Definitions for `show interface`

Entry	Definition
Packets Received Without Error	The total number of packets (including broadcast packets and multicast packets) received by the processor.
Packets Received With Error	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Broadcast Packets Received	The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.
Packets Transmitted Without Error	The total number of packets transmitted out of the interface.

TABLE 8-4 Entry Definitions for `show interface` *(Continued)*

Entry	Definition
Transmit Packets Errors	The number of outbound packets that could not be transmitted because of errors.
Collisions Frames	The best estimate of the total number of collisions on this Ethernet segment.
Time Since Counters Last Cleared	The elapsed time, in days, hours, minutes, and seconds since the statistics for this port were last cleared.

The display parameters, when the argument is "switchport" is as follows.

TABLE 8-5 Entry Definitions for `show interface` *`switchport`*

Entry	Definition
Broadcast Packets Received	The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.
Packets Received With Error	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Packets Transmitted Without Error	The total number of packets transmitted out of the interface.
Broadcast Packets Transmitted	The total number of packets that higher-level protocols requested to be transmitted to the Broadcast address, including those that were discarded or not sent.
Transmit Packet Errors	The number of outbound packets that could not be transmitted because of errors.
Address Entries Currently In Use	The total number of Forwarding Database Address Table entries now active on the switch, including learned and static entries.
VLAN Entries Currently In Use	The number of VLAN entries presently occupying the VLAN table.
Time Since Counters Last Cleared	The elapsed time, in days, hours, minutes, and seconds since the statistics for this switch were last cleared.

show interface ethernet

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

Format	**`show interface ethernet`** *`{<slot/port>	switchport}`*
Mode	Privileged EXEC

When you specify a value for *`<slot/port>`*, the command displays the following information, separated by:

- Packets Received (TABLE 8-6)
- Packets Received Successfully (TABLE 8-7)
- Packets Received With MAC Errors (TABLE 8-8)
- Received Packets Not Forwarded (TABLE 8-9)
- Packets Transmitted Octets (TABLE 8-10)
- Packets Transmitted Successfully (TABLE 8-11)
- Transmit Errors (TABLE 8-12)
- Transmit Discards (TABLE 8-13)
- Protocol Statistics (TABLE 8-14)
- Dot1x Statistics (TABLE 8-15)

TABLE 8-6 Entry Definitions for `show interface ethernet` Packets Received

Entry	**Definition**
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).

TABLE 8-6 Entry Definitions for `show interface ethernet` Packets Received

Entry	Definition
Packets Received 256-511 Octets	The total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
Packets Received 512-1023 Octets	The total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
Packets Received 1024-1518 Octets	The total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).
Packets Received > 1522 Octets	The total number of packets received that were longer than 1522 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.
Packets RX and TX 64 Octets	he total number of packets (including bad packets) received and transmitted that were 64 octets in length (excluding framing bits but including FCS octets).
Packets RX and TX 65-127 Octets	The total number of packets (including bad packets) received and transmitted that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
Packets RX and TX 128-255 Octets	The total number of packets (including bad packets) received and transmitted that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
Packets RX and TX 256-511 Octets	The total number of packets (including bad packets) received and transmitted that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
Packets RX and TX 512-1023 Octets	The total number of packets (including bad packets) received and transmitted that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
Packets RX and TX 1024-1518 Octets	The total number of packets (including bad packets) received and transmitted that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).
Packets RX and TX 1519-1522 Octets	The total number of packets (including bad packets) received and transmitted that were between 1519 and 1522 octets in length inclusive (excluding framing bits but including FCS octets).

TABLE 8-6 Entry Definitions for `show interface ethernet` Packets Received

Entry	Definition
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.

TABLE 8-7 Entry Definitions for `show interface ethernet` Packets Received Successfully

Entry	Definition
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.

TABLE 8-8 Entry Definitions for `show interface ethernet` Packets Received With MAC Errors

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

TABLE 8-9 Entry Definitions for `show interface ethernet` Received Packets Not Forwarded

Entry	Definition
Total	A count of valid frames received which were discarded (in other words, filtered) by the forwarding process.
Local Traffic Frames	The total number of frames dropped in the forwarding process because the destination address was located off of this port.
802.3x Pause Frames Received	A count of MAC Control frames received on this interface with an opcode indicating the PAUSE operation. This counter does not increment when the interface is operating in half-duplex mode.
Unacceptable Frame Type	The number of frames discarded from this port due to being an unacceptable frame type.

TABLE 8-9 Entry Definitions for `show interface ethernet` Received Packets Not Forwarded *(Continued)*

Entry	Definition
Multicast Tree Viable Discards	The number of frames discarded when a lookup in the multicast tree for a VLAN occurs while that tree is being modified.
Reserved Address Discards	The number of frames discarded that are destined to an IEEE 802.1 reserved address and are not supported by the system.
Broadcast Storm Recovery	The number of frames discarded that are destined for FF:FF:FF:FF:FF:FF when Broadcast Storm Recovery is enabled.
CFI Discards	The number of frames discarded that have CFI bit set and the addresses in RIF are in non-canonical format.
Upstream Threshold	The number of frames discarded due to lack of cell descriptors available for that packet's priority level.

TABLE 8-10 Entry Definitions for `show interface ethernet` Packets Transmitted Octets

Entry	Definition
Total Bytes	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).

TABLE 8-10 Entry Definitions for `show interface ethernet` Packets Transmitted Octets *(Continued)*

Entry	Definition
Packets Transmitted 512-1023 Octets	The total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
Packets Transmitted 1024-1518 Octets	The total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).
Max Frame Size	The maximum size of the Info (non-MAC) field that this port will receive or transmit.

TABLE 8-11 Entry Definitions for `show interface ethernet` Packets Transmitted Successfully

Entry	Definition
Total	The number of frames that have been transmitted by this port to its segment.
Unicast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
Multicast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to a Multicast address, including those that were discarded or not sent.
Broadcast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to the Broadcast address, including those that were discarded or not sent.

TABLE 8-12 Entry Definitions for `show interface ethernet` Transmit Errors

Entry	Definition
Total Errors	The sum of Single, Multiple, and Excessive Collisions.

TABLE 8-12 Entry Definitions for `show interface ethernet` Transmit Errors

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

TABLE 8-13 Entry Definitions for `show interface ethernet` Transmit Discards

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

TABLE 8-14 Entry Definitions for `show interface ethernet` Protocol Statistics

Entry	Definition
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.

TABLE 8-14 Entry Definitions for `show interface ethernet` Protocol Statistics

Entry	Definition
GMRP PDUs Received	The count of GMRP PDU's received in the GARP layer.
GMRP PDUs Transmitted	The count of GMRP PDU's transmitted from the GARP layer.
GMRP Failed Registrations	The number of times attempted GMRP registrations could not be completed.
STP BPDUs Transmitted	Spanning Tree Protocol Bridge Protocol Data Units sent
STP BPDUs Received	Spanning Tree Protocol Bridge Protocol Data Units received
RST BPDUs Transmitted	Rapid Spanning Tree Protocol Bridge Protocol Data Units sent
RSTP BPDUs Received	Rapid Spanning Tree Protocol Bridge Protocol Data Units received
MSTP BPDUs Transmitted	Multiple Spanning Tree Protocol Bridge Protocol Data Units sent
MSTP BPDUs Received	Multiple Spanning Tree Protocol Bridge Protocol Data Units received

TABLE 8-15 Entry Definitions for `show interface ethernet` Dotlx Statistics

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

When you use the *switchport* keyword, the following information appears.

TABLE 8-16 Entry Definitions for `show interface ethernet` *`switchport`*

Entry	Definition
Octets Received	The total number of octets of data received by the processor (excluding framing bits but including FCS octets).
Total Packets Received Without Error	The total number of packets (including broadcast packets and multicast packets) received by the processor.
Unicast Packets Received	The number of subnetwork-unicast packets delivered to a higher-layer protocol.
Multicast Packets Received	The total number of packets received that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address.
Broadcast Packets Received	The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.
Receive Packets Discarded	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. A possible reason for discarding a packet could be to free up buffer space.
Octets Transmitted	The total number of octets transmitted out of the interface, including framing characters.
Packets Transmitted without Errors	The total number of packets transmitted out of the interface.
Unicast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
Multicast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to a Multicast address, including those that were discarded or not sent.
Broadcast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to the Broadcast address, including those that were discarded or not sent.
Transmit Packets Discarded	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. A possible reason for discarding a packet could be to free up buffer space.
Most Address Entries Ever Used	The highest number of Forwarding Database Address Table entries that have been learned by this switch since the most recent reboot.

TABLE 8-16 Entry Definitions for `show interface ethernet` *`switchport`*

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

show mac-addr-table

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

Format	**`show mac-addr-table`** *`[<macaddr>	all]`*
Mode	Privileged EXEC

TABLE 8-17 Entry Definitions for `show mac-addr-table`

Entry	Definition
Mac Address	A unicast MAC address for which the switch has forwarding and or filtering information. The format is 6 or 8 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB. In an IVL system the MAC address will be displayed as 8 bytes.
Interface	The port which this address was learned.
Interface Index	This object indicates the ifIndex of the interface table entry associated with this port.

TABLE 8-17 Entry Definitions for `show mac-addr-table` *(Continued)*

Entry	Definition
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.

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.

Format	**`show running-config`** *`[all	<scriptname>]`*
Mode	Privileged EXEC

show sysinfo

This command displays switch information.

Format	**`show sysinfo`**
Mode	Privileged EXEC

TABLE 8-18 Entry Definitions for `show sysinfo`

Entry	Definition
Switch Description	Text used to identify this switch.
System Name	Name used to identify the switch.The factory default is blank. To configure the system name, see "snmp-server" on page 502.
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 502.
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 502.
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.
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:

- **`show version`**
- **`show sysinfo`**
- **`show port all`**
- **`show logging`**
- **`show event log`**
- **`show logging buffered`**

- **`show trap log`**
- **`show running config`**

Format	**`show tech-support`**
Mode	Privileged EXEC

Logging Commands

This section describes the commands you use to configure system logging, and to view logs and the logging settings.

`logging buffered`

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

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 console

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

Default	disabled; critical when enabled
Format	**`logging console`** *`[severitylevel]`*
Mode	Global Config

no logging console

This command disables logging to the console.

Format	**`no logging console`**
Mode	Global Config

logging host

This command enables logging to a host. You can configure up to eight hosts. The *<ipaddr>* is the IP address of the logging host. The *<port>* value is a port number from 1 to 65535. You can specify the *<severitylevel>* value as either an integer from 0 to 7 or symbolically through one of the following keywords: **emergency** (0), **alert** (1), **critical** (2), **error** (3), **warning** (4), **notice** (5), **info** (6), or **debug** (7).

Default	port—514 level—critical (2)
Format	**logging host** *<ipaddr> [<port>][<severitylevel>]*
Mode	Global Config

logging host remove

This command disables logging to host. See "show logging hosts" on page 443 for a list of host indexes.

Format	**logging host remove** *<hostindex>*
Mode	Global Config

logging port

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

Default	514
Format	**logging port** *<portid>*
Mode	Global Config

no logging port

This command resets the local logging port to the default.

Format	**`no logging port`**
Mode	Global Config

logging syslog

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

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

TABLE 8-19 Entry Definitions for `show logging`

Entry	Definition
Logging Client Local Port	Port on the collector/relay to which syslog messages are sent.
CLI Command Logging	Shows whether CLI Command logging is enabled.
Console Logging	Shows whether console logging is enabled.
Console Logging Severity Filter	The minimum severity to log to the console log. Messages with an equal or lower numerical severity are logged.
Buffered Logging	Shows whether buffered logging is enabled.
Syslog Logging	Shows whether syslog logging is enabled.
Log Messages Received	Number of messages received by the log process. This includes messages that are dropped or ignored.
Log Messages Dropped	Number of messages that could not be processed due to error or lack of resources.
Log Messages Relayed	Number of messages sent to the collector/relay.

show logging buffered

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

Format	**`show logging buffered`**
Mode	Privileged EXEC

TABLE 8-20 Entry Definitions for `show logging buffered`

Entry	Definition
Buffered (In-Memory) Logging	Shows whether the In-Memory log is enabled or disabled.
Buffered Logging Wrapping Behavior	The behavior of the In Memory log when faced with a log full situation.
Buffered Log Count	The count of valid entries in the buffered log.

show logging hosts

This command displays all configured logging hosts.

Format	**`show logging hosts`**
Mode	Privileged EXEC

TABLE 8-21 Entry Definitions for `show logging hosts`

Entry	Definition
Host Index	(Used for deleting hosts)
IP Address	IP address of the logging host.
Severity Level	The minimum severity to log to the specified address. The possible values are emergency (0), alert (1), critical (2), error (3), warning (4), notice (5), info (6), or debug (7).
Port	Displays the server port number, which is the port on the local host from which syslog messages are sent.
Host Status	The state of logging to configured syslog hosts. If the status is disable, no logging occurs.

show logging traplogs

This command displays SNMP trap events and statistics.

Format	**`show logging traplogs`**
Mode	Privileged EXEC

TABLE 8-22 Entry Definitions for `show logging traplogs`

Entry	Definition
Number of Traps Since Last Reset	Shows the number of traps since the last boot.
Trap Log Capacity	Shows the number of traps the system can retain.
Number of Traps Since Log Last Viewed	Shows the number of new traps since the command was last executed.

TABLE 8-22 Entry Definitions for `show logging traplogs` *(Continued)*

Entry	Definition
Log	Shows the log number.
System Time Up	Shows how long the system had been running at the time the trap was sent.
Trap	Shows the text of the trap message.

System Utility and Clear Commands

This section describes the commands you use to help troubleshoot connectivity issues and to restore various configurations to their factory defaults.

`traceroute`

Use the **`traceroute`** command to discover the routes that packets actually take when traveling to their destination through the network on a hop-by-hop basis. The *`<ipaddr>`* value should be a valid IP address. The *`[<port>]`* value should be a valid decimal integer in the range of 0 (zero) to 65535. The optional port parameter is the UDP port used as the destination of packets sent as part of the traceroute. This port should be an unused port on the destination system. The default value is 33434.

Format	**`traceroute`** *`<ipaddr> [<port>]`*
Mode	Privileged EXEC

`clear config`

This command resets the configuration to the factory defaults without powering off the switch. When you issue this command, a prompt appears to confirm that the reset should proceed. When you enter **`y`**, you automatically reset the switch.

Format	**`clear config`**
Mode	Privileged EXEC

clear counters

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

Format	**`clear counters`** *`{<slot/port> | all}`*
Mode	Privileged EXEC

clear igmpsnooping

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

Format	**`clear igmpsnooping`**
Mode	Privileged EXEC

clear pass

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

Format	**`clear pass`**
Mode	Privileged EXEC

clear port-channel

This command clears all port-channels (LAGs).

Format	**`clear port-channel`**
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.

Format	**`clear vlan`**
Mode	Privileged EXEC

enable passwd

This command prompts you to change the Privileged EXEC password. Passwords are a maximum of eight alphanumeric characters. The password is case sensitive.

Format	**`enable passwd`**
Mode	User 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`

This command checks if another computer is on the network and listens for connections. To use this command, configure the switch for network (in-band) connection. The source and target devices must have the ping utility enabled and running on top of TCP/IP. You can ping the switch from any IP workstation the switch is connected to 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.

Format	**`ping`** *`<ipaddr>`*
Modes	Privileged EXEC User EXEC

`quit`

This command closes the current telnet connection or resets the current serial connection. The system asks you whether to save configuration changes before quitting.

Format	**`quit`**
Modes	Privileged EXEC User EXEC

`reload`

This command resets the switch without powering it off. Reset means that all network connections are terminated and the boot code executes. The switch uses the stored configuration to initialize the switch. You are prompted to confirm that the reset should proceed. The LEDs on the switch indicate a successful reset.

Format	**`reload`**
Mode	Privileged EXEC

copy

The **copy** command uploads and downloads files to and from the switch. You can also use the copy command to manage the dual images (*image1* and *image2*) on the file system. Upload and download files from a server by using TFTP or Xmodem. Replace the *<source>* and *<destination>* parameters with the options in

Format	**copy** *<source> <destination>*
Mode	Privileged EXEC

Table 8-23. For the *<url>* source or destination, use one of the following values:

```
{xmodem | tftp://<ipaddr>/<filepath>/<filename>}
```

For TFTP, the *<ipaddr>* parameter is the IP address of the server, *<filepath>* is the path to the file, and *<filename>* is the name of the file you want to upload or download.

TABLE 8-23 Copy Parameters

Source	Destination	Description
nvram:clibanner	*<url>*	Copies the CLI banner to a server.
nvram:errorlog	*<url>*	Copies the error log file to a server.
nvram:log	*<url>*	Copies the log file to a server.
nvram:script <scriptname>	*<url>*	Copies a specified configuration script file to a server.
nvram:startup-config	*<url>*	Copies the startup configuration to a server.
nvram:traplog	*<url>*	Copies the trap log file to a server.
system:running-config	*nvram:startup-config*	Saves the running configuration to nvram.
<url>	*nvram:clibanner*	Downloads the CLI banner to the system.
<url>	*nvram:script <destfilename>*	Downloads a configuration script file to the system. During the download of a configuration script, the copy command validates the script. In case of any error, the command lists all the lines at the end of the validation process and prompts you to confirm before copying the script file.

TABLE 8-23 Copy Parameters *(Continued)*

Source	Destination	Description
<url>	*nvram:sshkey-dsa*	Downloads an SSH key file. For more information, see "Secure Shell (SSH) Command" on page 491.
<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 (HTTP) Commands" on page 495.
<url>	*nvram:sslpem-server*	Downloads an HTTP secure-server certificate.
<url>	*nvram:startup-config*	Downloads the startup configuration file to the system.
<url>	*nvram:system-image*	Downloads a code image to the system.
<url>	*{image1 | image2}*	Download an image from the remote server to either image.
{image1 | image2}	*<url>*	Upload either image to the remote server.
image1	*image2*	Copy `image1` to `image2`.
image2	*image1*	Copy `image2` to `image1`.

Simple Network Time Protocol (SNTP) Commands

This section describes the commands you use 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 16.

Default	6
Format	**`sntp broadcast client poll-interval`** *`<poll-interval>`*
Mode	Global Config

no sntp broadcast client poll-interval

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

Format	**`no sntp broadcast client poll-interval`**
Mode	Global Config

sntp client mode

This command enables Simple Network Time Protocol (SNTP) client mode and may set the mode to either broadcast or unicast.

Default	disabled
Format	**`sntp client mode`** *`[broadcast | unicast]`*
Mode	Global Config

no sntp client mode

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

Format	**`no sntp client mode`**
Mode	Global Config

sntp client port

This command sets the SNTP client port id to a value from 1-65535.

Default	123
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 16.

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 will set 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 multicast client poll-interval

This command will set the poll interval for SNTP multicast clients in seconds as a power of two where *`<poll-interval>`* can be a value from 6 to 16.

Default	6
Format	**`sntp multicast client poll-interval`** *`<poll-interval>`*
Mode	Global Config

no sntp multicast client poll-interval

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

Format	**`no sntp multicast client poll-interval`**
Mode	Global Config

sntp server

This command configures an SNTP server (a maximum of three). 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> [<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>`*
Mode	Global Config

`show sntp`

This command is used to display SNTP settings and status.

Format	**`show sntp`**
Mode	Privileged EXEC

TABLE 8-24 Entry Definitions for `show sntp`

Entry	Definition
Last Update Time	Time of last clock update.
Last Attempt Time	Time of last transmit query (in unicast mode).
Last Attempt Status	Status of the last SNTP request (in unicast mode) or unsolicited message (in broadcast mode).
Broadcast Count	Current number of unsolicited broadcast messages that have been received and processed by the SNTP client since last reboot.
Multicast Count	Current number of unsolicited multicast 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

TABLE 8-25 Entry Definitions for `show sntp client`

Entry	Definition
Client Supported Modes	Supported SNTP Modes (Broadcast, Unicast, or Multicast).
SNTP Version	The highest SNTP version the client supports
Port	SNTP Client Port
Client Mode	Configured SNTP Client Mode
Poll Interval	Poll interval value for SNTP clients in seconds as a power of two.
Poll Timeout	Poll timeout value in seconds for SNTP clients.
Poll Retry	Poll retry value for SNTP clients.

`show sntp server`

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

Format	**`show sntp server`**
Mode	Privileged EXEC

TABLE 8-26 Entry Definitions for `show sntp server`

Entry	Definition
Server IP Address	IP Address of configured SNTP Server
Server Type	Address Type of Server.
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.

TABLE 8-26 Entry Definitions for `show sntp server` *(Continued)*

Entry	Definition
Server Maximum Entries	Total number of SNTP Servers allowed.
Server Current Entries	Total number of SNTP configured. For each configured server, the following is displayed.
IP Address	IP Address of configured SNTP Server.
Address Type	Address Type of configured SNTP server.
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.

DHCP Server Commands

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

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

Default	ethernet
Format	**`hardware-address`** *`<hardwareaddress> <type>`*
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 1439. *`Minutes`* is an integer from 0 to 86399.

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.

Default	none
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

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 Dynamic Host Configuration Protocol (DHCP) clients.type Specifies the NetBIOS node type. Valid types are as follows:

- 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 white 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. Low-address and high-address are valid IP addresses; each made up of four decimal bytes ranging from 0 to 255. IP address 0.0.0.0 is invalid.

Default	none
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. Low-address and high-address are valid IP addresses; each made up of four decimal bytes ranging from 0 to 255. IP address 0.0.0.0 is invalid.

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 prevents the server from pinging pool addresses and sets the number of packets to 0.

Default	0
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 DHCP server.

Default	enabled
Format	**`ip dhcp conflict logging`**
Mode	Global Config

no ip dhcp conflict logging

This command disables conflict logging on 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. *<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.

Default	none
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

TABLE 8-27 Entry Definitions for `show ip dhcp binding`

Entry	Definition
IP address	The IP address of the client.
Hardware Address	The MAC Address or the client identifier.
Lease expiration	The lease expiration time of the IP Address assigned to the client.
Type	The 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

TABLE 8-28 Entry Definitions for `show ip dhcp global configuration`

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

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

TABLE 8-29 Entry Definitions for `show ip dhcp pool configuration`

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:
Network	The network number and the mask for the DHCP address pool. The following additional fields are displayed for Manual pool type.
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

TABLE 8-30 Entry Definitions for `show ip dhcp server statistics`

Entry	Definition
Automatic Bindings	The number of IP addresses that have been automatically mapped to the MAC addresses of hosts that are found in the DHCP database.
Expired Bindings	The number of expired leases.
Malformed Bindings	The number of truncated or corrupted messages that were received by the DHCP server. The following is displayed for Message Received.
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. The following is displayed for Message Sent:
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

TABLE 8-31 Entry Definitions for `show ip dhcp conflict`

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

DHCP Filtering

You can configure the DHCP Filtering feature as a security measure against unauthorized DHCP servers. DHCP filtering works by allowing you to configure each port as either a trusted port or an untrusted port. To optimize the DHCP filtering feature, configure the port that is connected to an authorized DHCP server on your network as a trusted port. Any DHCP responses received on a trusted port are forwarded. Make sure that all other ports are untrusted so that any DHCP (or BootP) responses received are discarded.

You can configure DHCP filtering on physical ports and LAGs. DHCP filtering is not operable on VLAN interfaces.

ip dhcp filtering

This command enables DHCP filtering globally.

Default	disabled
Format	**`ip dhcp filtering`**
Mode	Global Config

no ip dhcp filtering

This command disables DHCP filtering.

Format	**`no ip dhcp filtering`**
Mode	Global Config

ip dhcp filtering trust

This command configures an interface as trusted.

Default	untrusted
Format	**`ip dhcp filtering trust`**
Mode	Interface Config

no ip dhcp filtering trust

This command returns an interface to the default value for DHCP filtering.

Format	**`no ip dhcp filtering trust`**
Mode	Interface Config

show ip dhcp filtering

This command displays the DHCP filtering configuration.

Format	**`show ip dhcp filtering`**
Mode	Privileged EXEC

TABLE 8-32 Entry Definitions for `show ip dhcp filtering`

Entry	**Definition**
Interface	Specifies the interface by slot/port.
Trusted	Indicates whether the interface is trusted or untrusted.

CHAPTER 9

Management Commands

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

The commands in this chapter are divided into three 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.

This chapter contains the following sections:

Network Interface Commands

This section describes the commands you use to configure a logical interface for management access. To configure the management VLAN, see "network mgmt_vlan" on page 55

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

serviceport ip

This command sets the IP address, the netmask and the gateway of the network management port.

Format	**`serviceport ip`** *`<ipaddr> <netmask> [gateway]`*
Mode	Privileged EXEC

serviceport protocol

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

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

`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.

Format	**`network parms`** *`<ipaddr> <netmask> [<gateway>]`*
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 modify this value, the change is effective immediately. If you use the *`bootp`* parameter, the switch periodically sends requests to a BootP server until a response is received. If you use the *`dhcp`* parameter, the switch periodically sends requests to a DHCP server until a response is received. If you use the *`none`* parameter, you must configure the network information for the switch manually.

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

`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 EXE

network javamode

This command specifies whether or not 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, the user 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.

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

TABLE 9-1 Entry Definitions for `show network`

Entry	Definition
IP Address	The IP address of the interface. The factory default value is 0.0.0.0
Subnet Mask	The IP subnet mask for this interface. The factory default value is 0.0.0.0
Default Gateway	The default gateway for this IP interface. The factory default value is 0.0.0.0
Burned In MAC Address	The burned in MAC address used for in-band connectivity.
Locally Administered MAC Address	If desired, a locally administered MAC address can be configured for in-band connectivity. To take effect, 'MAC Address Type' must be set to 'Locally Administered'. Enter the address as twelve hexadecimal digits (6 bytes) with a colon between each byte. Bit 1 of byte 0 must be set to a 1 and bit 0 to a 0, i.e. byte 0 should have the following mask 'xxxx xx10'. The MAC address used by this bridge when it must be referred to in a unique fashion. It is recommended that this be the numerically smallest MAC address of all ports that belong to this bridge. However it is only required to be unique. When concatenated with dot1dStpPriority a unique BridgeIdentifier is formed which is used in the Spanning Tree Protocol.
MAC Address Type	Specifies which MAC address 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.
Network Configuration Protocol Current	Indicates which network protocol is being used. The options are bootp | dhcp | none.
Java Mode	Specifies if the switch should allow access to the Java applet in the header frame. Enabled means the applet can be viewed. The factory default is disabled.
Web Mode	Specifies if the switch should allow access to the Web Interface.

`show serviceport`

This command displays service port configuration information.

Format	**`show serviceport`**
Mode	Privileged EXEC

TABLE 9-2 Entry Definitions for `show serviceport`

Entry	**Definition**
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
ServPort Configuration Protocol Current	Indicates what network protocol was used on the last, or current power-up cycle, if any.
Burned in MAC Address	The burned in MAC address used for in-band connectivity.

Console Port Access Commands

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

`configuration`

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

Format	**`configuration`**
Mode	Privileged EXEC

lineconfig

This command gives you access to the Line Config mode, which allows you to configure various Telnet settings and the console port.

Format	**`lineconfig`**
Mode	Global Config

serial location

This command specifies whether the serial management port goes out the front or the RTM.

Default	front
Format	**`serial location`** *`{front	rtm}`*
Mode	Line Config

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

TABLE 9-3 Entry Definitions for `show serial`

Entry	Definition
Serial Port Login Timeout (minutes)	Specifies the time, in minutes, of inactivity on a Serial port connection, after which the Switch will close the connection. Any numeric value between 0 and 160 is allowed, the factory default is 5. A value of 0 disables the timeout.
Baud Rate (bps)	The default baud rate at which the serial port will try to connect. The available values are 1200, 2400, 4800, 9600, 19200, 38400,57600, and 115200 baud. The factory default is 9600 baud.
Character Size (bits)	The number of bits in a character. The number of bits is always 8.

TABLE 9-3 Entry Definitions for `show serial` *(Continued)*

Entry	Definition
Flow Control	Whether Hardware Flow-Control is enabled or disabled. Hardware Flow Control is always disabled.
Stop Bits	The number of Stop bits per character. The number of Stop bits is always 1.
Parity Type	The Parity Method used on the Serial Port. The Parity Method is always None.

Telnet Commands

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

`ip telnet server enable`

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

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

`no ip telnet server enable`

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

Format	**`no ip telnet server enable`**
Mode	Privileged EXEC

telnet

This command establishes a new outbound Telnet connection to a remote host. The *host* value must be a valid IP address. 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 *noecho* option disables local echo.

Format	**`telnet`** *`<host> <port> [debug] [line] [noecho]`*
Modes	Privileged EXEC User EXEC

transport input telnet

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

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

Default	enabled
Format	**`transport input telnet`**
Mode	Line Config

no transport input telnet

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

Format	**`no transport input telnet`**
Mode	Line Config

transport output telnet

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

Default	enabled
Format	**`transport output telnet`**
Mode	Line Config

no transport output telnet

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

Format	**`no transport output telnet`**
Mode	Line Config

session-limit

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

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

no session-limit

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

Format	**`no session-limit`**
Mode	Line Config

session-timeout

This command sets the Telnet session timeout value.The timeout value unit of time is minutes. A value of 0 indicates that a session remains active indefinitely.

Default	0
Format	**`session-timeout`** *<0-160>*
Mode	Line Config

no session-timeout

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

Format	**`no session-timeout`**
Mode	Line Config

telnetcon maxsessions

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

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

no telnetcon maxsessions

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

Format	**`no telnetcon maxsessions`**
Mode	Privileged EXEC

telnetcon timeout

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

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

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

no telnetcon timeout

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

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

Format	**`no telnetcon timeout`**
Mode	Privileged EXEC

disconnect

Use the **`disconnect`** command to close Telnet or SSH sessions. Use *`all`* to close all Telnet and SSH 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

`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

TABLE 9-4 Entry Definitions for `show telnet`

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

`show telnetcon`

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

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

TABLE 9-5 Entry Definitions for `show telnetcon`

Entry	Definition
Remote Connection Login Timeout (minutes)	This object indicates the number of minutes a remote connection session is allowed to remain inactive before being logged off. May be specified as a number from 1 to 160. The factory default is 5.
Maximum Number of Remote Connection Sessions	This object indicates the number of simultaneous remote connection sessions allowed. The factory default is 5.
Allow New Telnet Sessions	Indicates that new Telnet sessions will not be allowed when set to no. The factory default value is yes.

Secure Shell (SSH) Command

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

Note – The system allows a maximum of 5 SSH sessions.

`ip ssh`

Use this command to enable SSH access to the system.

Default	disabled
Format	**`ip ssh`**
Mode	Privileged EXEC

no ip ssh

Use this command to disable SSH access to the system.

Format	**`no ip ssh`**
Mode	Privileged EXEC

ip ssh protocol

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

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

ip ssh server enable

This command enables the IP secure shell server.

Default	disabled
Format	**`ip ssh server enable`**
Mode	Privileged EXEC

no ip ssh server enable

This command disables the IP secure shell server.

Format	**`no ip ssh server enable`**
Mode	Privileged EXEC

sshcon maxsessions

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

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

no sshcon maxsessions

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

Format	**`no sshcon maxsessions`**
Mode	Privileged EXEC

sshcon timeout

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

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

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

no sshcon timeout

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

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

Format	**`no sshcon timeout`**
Mode	Privileged EXEC

`show ip ssh`

This command displays the ssh settings.

Format	**`show ip ssh`**
Mode	Privileged EXEC

TABLE 9-6 Entry Definitions for `show ip ssh`

Entry	Definition
Administrative Mode	This field indicates whether the administrative mode of SSH is enabled or disabled.
Protocol Level	The protocol level may have the values of version 1, version 2 or both versions 1 and version 2.
Connections	This field specifies the current SSH connections.

Hypertext Transfer Protocol (HTTP) Commands

This section describes the commands you use to configure 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 secure-port

This command is used to set the SSL port where port can be 1-65535 and the default is port 443.

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

no ip http secure-port

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

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

ip http secure-protocol

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

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

ip http secure-server

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

Default	disabled
Format	**`ip http secure-server`**
Mode	Privileged EXEC

no ip http secure-server

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

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

ip http server

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

Disabling the Web interface takes effect immediately. All interfaces are effected.

Default	enabled
Format	**`ip http server`**
Mode	Privileged EXEC

no ip http server

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

Format	**`no ip http server`**
Mode	Privileged EXEC

show ip http

This command displays the http settings for the switch.

Format	**`show ip http`**
Mode	Privileged EXEC

TABLE 9-7 Entry Definitions for `show ip http`

Entry	Definition
Secure-Server Administrative Mode	Indicates whether the administrative mode of secure HTTP is enabled or disabled.
Secure Protocol Level	Possible values are SSL3, TSL1, or both SSL3 and TSL1.
Secure Port	This field specifies the port configured for SSLT.
HTTP Mode	This field indicates whether the HTTP mode is enabled or disabled.

User Account Commands

This section describes the commands you use to add, manage, and delete system users. FASTPATH 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, and there is only one user allowed with read/write privileges. You can configure up to five read-only users on the system.

users name

This command adds a new user account, if space permits. The account *`<username>`* can be up to eight characters in length. You can use alphanumeric characters as well as the dash ('-') and underscore ('_'). You can define up to six user names.

Note – The *<username>* is not case sensitive when you add and delete users, and when the user logs in. However, when you use the *<username>* to set the user password, authentication, or encryption, you must enter the *<username>* in the same case you used when you added the user. To see the case of the *<username>*, enter the **`show users`** command.

Format	**`users name`** *<username>*
Mode	Global Config

no users name

This command removes a user account.

Format	**`no users name`** *<username>*
Mode	Global Config

Note – You cannot delete the "admin" user account.

users passwd

Use this command to change a password. Passwords are a maximum of eight alphanumeric characters. If a user is authorized for authentication or encryption is enabled, the password length must be at least eight alphanumeric characters. The password is case sensitive. When you change a password, a prompt asks for the old password. If there is no password, press enter. 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 password
Format	**`users passwd`** *<username>*
Mode	Global Config

no users passwd

This command sets the password of an existing user to blank. When you change a password, a prompt asks for the old password. If there is no password, press enter.

Format	**`no users passwd`** *`<username>`*
Mode	Global Config

users snmpv3 accessmode

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

Default	admin - readwrite other - readonly
Format	**`users snmpv3 accessmode`** *`<username> {readonly	readwrite}`*
Mode	Global Config

no users snmpv3 accessmode

This command sets the snmpv3 access privileges for the specified 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 users snmpv3 accessmode`** *`<username>`*
Mode	Global Config

users snmpv3 authentication

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

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

no users snmpv3 authentication

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

Format	**`no users snmpv3 authentication`** *`<username>`*
Mode	Global Config

users snmpv3 encryption

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

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

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

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

no users 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 users snmpv3 encryption`** *`<username>`*
Mode	Global Config

show loginsession

This command displays current Telnet and serial port connections to the switch.

Format	**`show loginsession`**
Mode	Privileged EXEC

TABLE 9-8

Entry	Definition
ID	Login Session ID
User Name	The name the user will use to login using the serial port or Telnet.
Connection From	IP address of the Telnet 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.

show users

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

Format	**`show users`**
Mode	Privileged EXEC

TABLE 9-9 Entry Definitions for `show users`

Entry	Definition
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 (Read/Write) or is only able to view them (Read Only). As a factory default, the "admin" user has Read/Write access and the "guest" has Read Only access. There can only be one Read/Write user and up to five Read Only users.
SNMPv3 Access Mode	This field displays the SNMPv3 Access Mode. If the value is set to **`ReadWrite,`** the SNMPv3 user 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	This field displays the authentication protocol to be used for the specified login user.
SNMPv3 Encryption	This field displays the encryption protocol to be used for the specified login user.

SNMP Commands

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

snmp-server

This command sets the name and the physical location of the switch, and the organization responsible for the network. The range for *`<name>`*, *`<loc>`* and *`<con>`* is from 1 to 31 alphanumeric characters.

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

snmp-server community

This command adds (and names) a new SNMP community. A community *<name>* is a name associated with the switch and with a set of SNMP managers that manage it with a specified privileged level. The length of *<name>* can be up to 16 case-sensitive characters.

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

Default	public and private, which you can rename default values for the remaining four community names are blank
Format	**`snmp-server community`** *<name>*
Mode	Global Config

no snmp-server community

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

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

snmp-server community ipaddr

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

Default	0.0.0.0
Format	**`snmp-server community ipaddr`** *<ipaddr> <name>*
Mode	Global Config

no snmp-server community ipaddr

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

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

snmp-server community ipmask

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

Default	0.0.0.0
Format	**`snmp-server community ipmask`** *`<ipmask> <name>`*
Mode	Global Config

no snmp-server community ipmask

This command sets a client IP mask for an SNMP community to 0.0.0.0. The name is the applicable community name. The community name may be up to 16 alphanumeric characters.

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

snmp-server community mode

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

Default	private and public communities - enabled other four - disabled
Format	**`snmp-server community mode`** *`<name>`*
Mode	Global Config

no snmp-server community mode

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

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

snmp-server community ro

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

Format	**`snmp-server community ro`** *`<name>`*
Mode	Global Config

snmp-server community rw

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

Format	**`snmp-server community rw`** *`<name>`*
Mode	Global Config

snmp-server enable traps violation

This command enables the sending of new violation traps designating when a packet with a disallowed MAC address is received on a locked port.

Note – For other port security commands, see "Protected Ports Commands" on page 75.

Default	disabled
Format	**`snmp-server enable traps violation`**
Mode	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 bcaststorm

This command enables the broadcast storm trap. When enabled, broadcast storm traps are sent only if the broadcast storm recovery mode setting associated with the port is enabled.

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

no snmp-server enable traps bcaststorm

This command disables the broadcast storm trap. When enabled, broadcast storm traps are sent only if the broadcast storm recovery mode setting associated with the port is enabled.

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

snmp-server enable traps linkmode

This command enables Link Up/Down traps for the entire switch. When enabled, link traps are sent only if the Link Trap flag setting associated with the port is enabled. See "snmp trap link-status" on page 511.

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

snmptrap

This command adds an SNMP trap receiver. The maximum length of *<name>* is 16 case-sensitive alphanumeric characters. The *<snmpversion>* is the version of SNMP. The version parameter options are snmpv1 or snmpv2.

Note – The *<name>* parameter does not need to be unique, however; the *<name>* and *<ipaddr>* pair must be unique. Multiple entries can exist with the same *<name>*, as long as they are associated with a different *<ipaddr>*. The reverse scenario is also acceptable. The *<name>* is the community name used when sending the trap to the receiver, but the *<name>* is not directly associated with the SNMP Community Table, See "snmp-server community" on page39."

Default	snmpv2
Format	**`snmptrap`** *`<name> <ipaddr> [snmpversion <snmpversion>]`*
Mode	Global Config

no snmptrap

This command deletes trap receivers for a community.

Format	**`no snmptrap`** *`<name> <ipaddr>`*
Mode	Global Config

snmptrap snmpversion

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

Note – This command does not support a "no" form.

Default	snmpv2
Format	**`snmptrap snmpversion`** *`<name> <ipaddr> <snmpversion>`*
Mode	Global Config

snmptrap ipaddr

This command assigns an IP address to a specified community name. The maximum length of name is 16 case-sensitive alphanumeric characters.

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

Format	**`snmptrap ipaddr`** *`<name> <ipaddrold> <ipaddrnew>`*
Mode	Global Config

snmptrap mode

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

Format	**`snmptrap mode`** *`<name> <ipaddr>`*
Mode	Global Config

no snmptrap mode

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

Format	**`no snmptrap mode`** *`<name> <ipaddr>`*
Mode	Global Config

snmp trap link-status

This command enables link status traps by interface.

Note – This command is valid only when the Link Up/Down Flag is enabled. See "snmp-server enable traps linkmode" on page 508.

Format	**`snmp trap link-status`**
Mode	Interface Config

no snmp trap link-status

This command disables link status traps by interface.

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

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

snmp trap link-status all

This command enables link status traps for all interfaces.

Note – This command is valid only when the Link Up/Down Flag is enabled. See “snmp-server enable traps linkmode” on page 508.

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

no snmp trap link-status all

This command disables link status traps for all interfaces.

Note – This command is valid only when the Link Up/Down Flag is enabled. See “snmp-server enable traps linkmode” on page 508.

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

`show snmpcommunity`

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

The SNMP agent of the switch complies with SNMP Versions 1, 2 or 3. For more information about the SNMP specification, see the SNMP RFCs. The SNMP agent sends traps through TCP/IP to an external SNMP manager based on the SNMP configuration (the trap receiver and other SNMP community parameters).

Format	**`show snmpcommunity`**
Mode	Privileged EXEC

TABLE 9-10 Entry Definitions for `show snmpcommunity`

Entry	Definition
SNMP Community Name	The community string to which this entry grants access. A valid entry is a case-sensitive alphanumeric string of up to 16 characters. Each row of this table must contain a unique community name.
Client IP Address	An IP address (or portion thereof) from which this device will accept SNMP packets with the associated community. The requesting entity's IP address is ANDed with the Subnet Mask before being compared to the IP Address. Note: If the Subnet Mask is set to 0.0.0.0, an IP Address of 0.0.0.0 matches all IP addresses. The default value is 0.0.0.0
Client IP Mask	A mask to be ANDed with the requesting entity's IP address before comparison with IP Address. If the result matches with IP Address then the address is an authenticated IP address. For example, if the IP Address = 9.47.128.0 and the corresponding Subnet Mask = 255.255.255.0 a range of incoming IP addresses would match, i.e. the incoming IP Address could equal 9.47.128.0 - 9.47.128.255. The default value is 0.0.0.0
Access Mode	The access level for this community string.
Status	The status of this community access entry.

show snmptrap

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

Format	**`show snmptrap`**
Mode	Privileged EXEC

TABLE 9-11 Entry Definitions for `show snmptrap`

SNMP Trap Name	The community string of the SNMP trap packet sent to the trap manager. The string is case sensitive and can be up to 16 alphanumeric characters.
IP Address	The IP address to receive SNMP traps from this device.
Status	Indicates the receiver's status (enabled or disabled).

show trapflags

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

Format	**`show trapflags`**
Mode	Privileged EXEC

TABLE 9-12 Entry Definitions for `show trapflags`

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

TABLE 9-12 Entry Definitions for `show trapflags` *(Continued)*

Entry	Definition
Spanning Tree Flag	Can be enabled or disabled. The factory default is enabled. Indicates whether spanning tree traps are sent.
Broadcast Storm Flag	Can be enabled or disabled. The factory default is enabled. Indicates whether broadcast storm traps are sent.
ACL Traps	May be enabled or disabled. The factory default is disabled. Indicates whether ACL traps are sent.
BGP4 Traps	Can be enabled or disabled. The factory default is disabled. Indicates whether BGP4 traps are sent.
DVMRP Traps	Can be enabled or disabled. The factory default is disabled. Indicates whether DVMRP traps are sent.
OSPF Traps	Can be enabled or disabled. The factory default is disabled. Indicates whether OSPF traps are sent.
PIM Traps	Can be enabled or disabled. The factory default is disabled. Indicates whether PIM traps are sent.

CLI Command Logging Command

This section describes the commands you use to configure CLI Command Logging.

`logging cli-command`

This command enables the CLI command logging feature, which enables the FASTPATH software to log all CLI commands issued on the system.

Default	enabled
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

RADIUS Commands

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

radius accounting mode

This command is used to enable the RADIUS accounting function.

Default	disabled
Format	**`radius accounting mode`**
Mode	Global Config

no radius accounting mode

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

Format	**`no radius accounting mode`**
Mode	Global Config

radius server host

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

Note – To re-configure 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 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 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 1 - 65535, with 1813 being the default.

Note – To re-configure a RADIUS accounting server to use the default UDP *<port>*, set the *<port>* parameter to 1813.

Format	**radius server host** *{auth | acct} <ipaddr> [<port>]*
Mode	Global Config

no radius server host

This command is used to remove the configured RADIUS authentication server or the RADIUS accounting server. 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>* parameter must match the IP address of the previously configured RADIUS authentication / accounting server.

Format	**`no radius server host`** *`{auth	acct} <ipaddress>`*
Mode	Global Config

radius server key

This command is used to configure the shared secret between the RADIUS client and the RADIUS accounting / authentication 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 provided must match a previously configured server. When this command is executed, the secret is prompted.

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

Format	**`radius server key`** *`{auth	acct} <ipaddr>`*
Mode	Global Config

radius server msgauth

This command enables the message authenticator attribute for a specified server.

Format	**`radius server msgauth`** *`<ipaddr>`*
Mode	Global Config

no radius server msgauth

This command disables the message authenticator attribute for a specified server.

Format	**`no radius server msgauth`** *`<ipaddr>`*
Mode	Global Config

radius server primary

This command is used to configure the primary RADIUS authentication server for this RADIUS client. The primary server handles RADIUS requests. The remaining configured servers are only used if the primary server cannot be reached. You can configure up to three servers on each client. Only one of these servers can be configured as the primary. If a primary server is already configured prior to this command being executed, the server specified by the IP address specified used in this command will become the new primary server. The IP address must match that of a previously configured RADIUS authentication server.

Format	**`radius server primary`** *`<ipaddr>`*
Mode	Global Config

radius server retransmit

This command sets the maximum number of times a request packet is re-transmitted when no response is received from the RADIUS server. The retries value is an integer in the range of 1 to 15.

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

no radius server retransmit

This command sets the maximum number of times a request packet is re-transmitted, to the default value.

Format	**`no radius server retransmit`**
Mode	Global Config

radius server timeout

This command sets 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

no radius server timeout

This command sets the timeout value to the default value.

Format	**`no radius server timeout`**
Mode	Global Config

show radius

This command is used to display the various RADIUS configuration items for the switch as well as the configured RADIUS servers. If the optional token 'servers' is not included, the following RADIUS configuration items are displayed.

Format	**`show radius`** *`[servers]`*
Mode	Privileged EXEC

TABLE 9-13 Entry Definitions for `show radius`

Entry	**Definition**
Primary Server IP Address	Shows the configured server currently in use for authentication.
Number of configured servers	The configured IP address of the authentication server.

TABLE 9-13 Entry Definitions for `show radius` *(Continued)*

Entry	Definition
Max number of retransmits	The configured value of the maximum number of times a request packet is retransmitted.
Timeout Duration	The configured timeout value, in seconds, for request re-transmissions.
Accounting Mode	Yes or No.

If you use the *`[servers]`* keyword, the following information displays.

IP Address	IP Address of the configured RADIUS server.
Port	The port in use by this server.

TABLE 9-14 Entry Definitions for `show radius` *`servers`*

Entry	Definition
Type	Primary or secondary.
Secret Configured	Yes / No.
Message Authenticator	The message authenticator attribute for the selected server, which can be enables or disables.

show radius accounting

This command is used to display the configured RADIUS accounting mode, accounting server and the statistics for the configured accounting server.

Format	**`show radius accounting`** *`[statistics <ipaddr>]`*
Mode	Privileged EXEC

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

TABLE 9-15 Entry Definitions for `show radius accounting`

Entry	Definition
Mode	Enabled or disabled
IP Address	The configured IP address of the RADIUS accounting server.
Port	The port in use by the RADIUS accounting server.
Secret Configured	Yes or No.

If you use the optional *`statistics <ipaddr>`* parameter, the statistics for the configured RADIUS accounting server are displayed. The IP address parameter must match that of a previously configured RADIUS accounting server. The following information regarding the statistics of the RADIUS accounting server is displayed.

TABLE 9-16 Entry Definitions for `show radius accounting` *`statistics`*

Entry	Definition
Accounting Server IP Address	IP Address of the configured RADIUS accounting server
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 the RADIUS accounting server.
Requests	The number of RADIUS Accounting-Request packets sent to this accounting 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 and 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.

TABLE 9-16 Entry Definitions for `show radius accounting` *`statistics`*

Entry	Definition
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.

`show radius statistics`

This command is used to display the statistics for RADIUS or configured server. To show the configured RADIUS server statistic, the IP Address specified must match that of a previously configured RADIUS server. On execution, the following fields are displayed.

Format	**`show radius statistics`** *`[<ipaddr>]`*
Mode	Privileged EXEC

If you do not specify the IP address, then only Invalid Server Address field is displayed. Otherwise other listed fields are displayed.

TABLE 9-17 Entry Definitions for `show radius statistics`

Entry	Definition
Invalid Server Addresses	The number of RADIUS Access-Response packets received from unknown addresses.
Server IP Address	IP Address of the Server.
Round Trip Time	The time interval, in hundredths of a second, between the most recent Access-Reply, Access-Challenge and the Access-Request that matched it from the RADIUS authentication server.
Access Requests	The number of RADIUS Access-Request packets sent to this server. This number does not include retransmissions.
Access Retransmission	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, which were received from this server.
Access Rejects	The number of RADIUS Access-Reject packets, including both valid and invalid packets, which were received from this server.

TABLE 9-17 Entry Definitions for `show radius statistics` *(Continued)*

Entry	Definition
Access Challenges	The number of RADIUS Access-Challenge packets, including both valid and invalid packets, which were received from this server.
Malformed Access Responses	The number of malformed RADIUS Access-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators or signature attributes or unknown types are not included as malformed access responses.
Bad Authenticators	The number of RADIUS Access-Response packets containing invalid authenticators or signature attributes received from this server.
Pending Requests	The number of RADIUS Access-Request packets destined for this server that have not yet timed out or received a response.
Timeouts	The number of authentication timeouts to this server.
Unknown Types	The number of RADIUS packets of unknown types, which 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.

TACACS+ Commands

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

tacacs-server host

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

Format	**`tacacs-server host`** *`<ip-address>`*
Mode	Global Config

no tacacs-server host

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

Format	**`no tacacs-server host`** *`<ip-address>`*
Mode	Global Config

tacacs-server key

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

Format	**`tacacs-server key`** *`<key-string>`*
Mode	Global Config

no tacacs-server key

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

Format	**`no tacacs-server key`** *`<key-string>`*
Mode	Global Config

tacacs-server timeout

Use the **`tacacs-server timeout`** command to set the timeout value for communication with the TACACS+ servers. The *`<timeout>`* parameter has a range of 1-30 and is the timeout value in seconds.

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

no tacacs-server timeout

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

Format	**`no tacacs-server timeout`**
Mode	Global Config

key

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

Format	**`key`** *`<key-string>`*
Mode	TACACS Config

port

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

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

`priority`

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

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

`timeout`

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

Format	**`timeout`** *`<timeout>`*
Mode	TACACS Config

`show tacacs`

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

Format	**`show tacacs`** *`[<ip-address>]`*
Mode	Privileged EXEC

TABLE 9-18 Entry Definitions for `show tacacs`

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

Configuration Scripting Commands

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

Use the **`show running-config`** command (see "show running-config" on page 436) to capture the running configuration into a script. Use the **`copy`** command (see "copy" on page 448) to transfer the configuration script to or from the switch.

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

Scripts must conform to the following rules:

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

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

The following lines show an example of a script:

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

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	Global Config

TABLE 9-19

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

The output format is as follows:

```
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

Pre-login Banner and System Prompt Commands

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

copy (pre-login banner)

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

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

Index