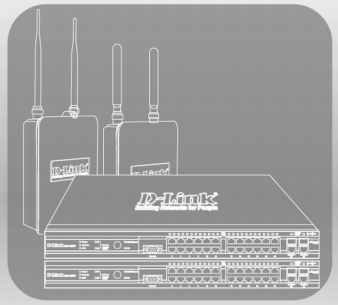
D-Link
Building Networks for People



CLI Command Reference

Product Model: DWS-4000 series
DWL-x600AP

Unified Wired and Wireless Access System

November 2011

Table of Contents

List of Tables

About This Document

This document describes command-line interface (CLI) commands you use to view and configure D-Link DWS-4000 Series software on a Unified Wired and Wireless Access System switch. You can access the CLI by using a direct connection to the serial port or by using telnet or SSH over a remote network connection.

Note: This document contains both standalone and stacking commands. The stacking commands are available on the DWS-4000 Series Unified Switch.

Audience

This document is for system administrators who configure and operate systems using DWS-4000 software. It provides an understanding of the configuration options of the DWS-4000 software.

Software engineers who integrate DWS-4000 software into their hardware platform can also benefit from a description of the configuration options.

This document assumes that the reader has an understanding of the DWS-4000 software base and has read the appropriate specification for the relevant networking device platform. It also assumes that the reader has a basic knowledge of Ethernet and networking concepts.

Refer to the release notes for the DWS-4000 application-level code. The release notes detail the platform-specific functionality of the Switching, Routing, SNMP, Configuration, Management, and other packages. The suite of features the DWS-4000 packages support is not available on all the platforms to which DWS-4000 software has been ported.

Acronyms and Abbreviations

In most cases, acronyms and abbreviations are defined on first use.

Document Conventions

This section describes the conventions this document uses.

Note: A note provides more information about a feature or technology.

Caution! A caution provides information about critical aspects of the configuration, combinations of settings, events, or procedures that can adversely affect network connectivity, security, and so on.

This guide uses the typographical conventions described in Table 1.

Table 1: Typographical Conventions

Symbol	*Description*	*Example*
Blue Text	Hyperlinked text.	See "About This Document" on page 11.
`courier font`	Command or command-line text	`show network`
`italic courier font`	`Variable value. You must replace the italicized text with an appropriate value, which might be a name or number.`	*value*
[] square brackets	`Optional parameter.`	`[value]`
{ } curly braces	Required parameter values. You must select a parameter from the list or range of choices.	`{choice1 | choice2}`
| Vertical bar	Separates the mutually exclusive choices.	`choice1 | choice2`
[{ }] Braces within square brackets	Optional parameter values. Indicates a choice within an optional element.	`[{choice1 | choice2}]`

Additional Documentation

The following documentation provides additional information about D-Link DWS-4000 Series software:

- The *D-Link DWS-4000 Series Administrator's Guide* describes the Web-based graphical user interface (GUI) for managing, monitoring, and configuring the switch. The *Administrator's Guide* also contains step-by-step configuration examples for several features.
- The *D-Link DWS-4000 Series Wired Configuration Guide* contains a variety of configuration examples that show how to configure the wired features on the switch.
- Release notes for this DWS-4000 Series product detail the platform-specific functionality of the software packages, including issues and workarounds.

About DWS-4000 Software

The DWS-4000 software has two purposes:

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

Scope

DWS-4000 software encompasses both hardware and software support. The software is partitioned to run in the following processors:

- CPU

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

- Networking device processor

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

Product Concept

Fast Ethernet and Gigabit Ethernet switching continues to evolve from high-end backbone applications to desktop switching applications. The price of the technology continues to decline, while performance and feature sets continue to improve. Devices that are capable of switching Layers 2, 3, and 4 are increasingly in demand. DWS-4000 software provides a flexible solution to these ever-increasing needs.

The exact functionality provided by each networking device on which the DWS-4000 software base runs varies depending upon the platform and requirements of the DWS-4000 software.

DWS-4000 software includes a set of comprehensive management functions for managing both DWS-4000 software and the network. You can manage the DWS-4000 software by using one of the following three methods:

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

Each of the DWS-4000 management methods enables you to configure, manage, and control the software locally or remotely using in-band or out-of-band mechanisms. Management is standards-based, with configuration parameters and a private MIB providing control for functions not completely specified in the MIBs.

Technical Support

D-Link provides customer access to the latest user documentation and software updates for D-Link products through its support website (http://support.dlink.com).

Section 1: Using the Command-Line Interface

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

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

Command Syntax

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

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

`network parms ipaddr netmask [gateway]`

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

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

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

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

Common Parameter Values

Parameter values might be names (strings) or numbers. To use spaces as part of a name parameter, enclose the name value in double quotes. For example, the expression “System Name with Spaces” forces the system to accept the spaces. Empty strings (““) are not valid user-defined strings. Table 2 describes common parameter values and value formatting.

Table 2: Parameter Descriptions

Parameter	*Description*

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

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

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

DWS-4000 software references physical entities such as cards and ports by using a slot/port naming convention. The DWS-4000 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 3: Type of Slots

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

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

Table 4: Type of Ports

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

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.

Using the *No* Form of a Command

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

DWS-4000 Modules

DWS-4000 software consists of flexible modules that can be applied in various combinations to develop advanced Layer 2/3/4+ products. The commands and command modes available on your switch depend on the installed modules. Additionally, for some `show` commands, the output fields might change based on the modules included in the DWS-4000 software.

The DWS-4000 software suite includes the following modules:

- Switching (Layer 2)
- Routing (Layer 3)
- IPv6—IPv6 routing
- Multicast
- Wireless
- Quality of Service
- Management (CLI, Web UI, and SNMP)
- IPv6 Management—Allows management of the DWS-4000 device through an IPv6 through an IPv6 address without requiring the IPv6 Routing package in the system. The management address can be associated with the network port (front-panel switch ports), a routine interface (port or VLAN) and the Service port.
- Stacking

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

Command Modes

The CLI groups commands into modes according to the command function. Each of the command modes supports specific DWS-4000 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 5 describes the command modes and the prompts visible in that mode.

Note: The command modes available on your switch depend on the software modules that are installed. For example, a switch that does not support stacking does not have the Stack Global Config Command Mode.

Table 5: CLI Command Modes

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

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

Line Console	`Switch (config-line)#`	Contains commands to configure outbound telnet settings and console interface settings, as well as to configure console login/enable authentication.
Line SSH	`Switch (config-ssh)#`	Contains commands to configure SSH login/ enable authentication.
Line Telnet	`Switch (config-telnet)#`	Contains commands to configure telnet login/ enable authentication.

Table 5: CLI Command Modes (Cont.)

Command Mode	*Prompt*	*Mode Description*
AAA IAS User Config	`Switch (Config-IAS-User)#`	Allows password configuration for a user in the IAS database.
Mail Server Config	`Switch (Mail-Server)#`	Allows configuration of the email server.
Policy Map Config	`Switch (Config-policy-map)#`	Contains the QoS Policy-Map configuration commands.
Policy Class Config	`Switch (Config-policy-class-map)#`	Consists of class creation, deletion, and matching commands. The class match commands specify Layer 2, Layer 3, and general match criteria.
Class Map Config	`Switch (Config-class-map)#`	Contains the QoS class map configuration commands for IPv4.
Ipv6_Class-Map Config	`Switch (Config-class-map)#`	Contains the QoS class map configuration commands for IPv6.
Router OSPF Config	`Switch (Config-router)#`	Contains the OSPF configuration commands.
Router OSPFv3 Config	`Switch (Config rtr)#`	Contains the OSPFv3 configuration commands.
Router RIP Config	`Switch (Config-router)#`	Contains the RIP configuration commands.
Router BGP Config	`Switch (Config-router)#`	Contains the BGP4 configuration commands.
MAC Access-list Config	`Switch (Config-mac-access-list)#`	Allows you to create a MAC Access-List and to enter the mode containing MAC Access-List configuration commands.
TACACS Config	`Switch (Tacacs)#`	Contains commands to configure properties for the TACACS servers.
DHCP Pool Config	`Switch (Config dhcp-pool)#`	Contains the DHCP server IP address pool configuration commands.
DHCPv6 Pool Config	`Switch (Config dhcp6-pool)#`	Contains the DHCPv6 server IPv6 address pool configuration commands.
Stack Global Config Mode	`Switch (Config stack)#`	Allows you to access the Stack Global Config Mode.
ARP Access-List Config Mode	`Switch (Config-arp-access-list)#`	Contains commands to add ARP ACL rules in an ARP Access List.
Wireless Config Mode	`Switch (Config-wireless)#`	Contains global WLAN switch configuration commands and provides access to other WLAN command modes.
AP Config Mode	`Switch (Config-ap)#`	Contains commands to configure entries in the local AP database, which is used for AP validation.
AP Profile Config Mode	`Switch (Config-ap-profile)#`	Contains commands to configure the default AP profile settings as well as settings for new AP profile.
AP Profile Radio Config Mode	`Switch (Config-ap-profile-radio)#`	Contains commands to modify the radio configuration parameters for an AP profile.

Table 5: CLI Command Modes (Cont.)

Command Mode	*Prompt*	*Mode Description*
AP Profile VAP Config Mode	`Switch (Config-ap-profile-vap)#`	Contains commands to configure radio 1 or radio 2 within an AP profile.
Network Config Mode	`Switch (Config-network)#`	Contains commands to configure WLAN settings for up to 64 different networks.
ARP Access-List Config Mode	`Switch (Config-arp-access-list)#`	Contains commands to add ARP ACL rules in an ARP Access List.
Captive Portal Config Mode	`Switch (Config-CP)#`	Contains commands to configure global captive portal settings.
Captive Portal Instance Mode	`Switch (Config-CP 1)#`	Contains commands to configure a captive portal instance.
WDS AP Group Config Mode	`Switch (Config-WDS-group)#`	Contains commands to modify the configuration parameters of a WDS-managed AP group.
Device Location Building Config Mode	Switch (Config-building)#	Contains commands to specify the location of a WLAN device.
Device Location Floor Config Mode	Switch (Config-building-floor)#	Contains commands to specify the location of a WLAN device.

Table 6 explains how to enter or exit each mode.

Table 6: CLI Mode Access and Exit

Command Mode	*Access Method*	*Exit or Access Previous Mode*
User EXEC	This is the first level of access.	To exit, enter `logout`.
Privileged EXEC	From the User EXEC mode, enter `enable`.	To exit to the User EXEC mode, enter `exit` or press `Ctrl-Z`.
Global Config	From the Privileged EXEC mode, enter `configure`.	To exit to the Privileged EXEC mode, enter `exit`, or press `Ctrl-Z`.
VLAN Config	From the Privileged EXEC mode, enter `vlan database`.	To exit to the Privileged EXEC mode, enter `exit`, or press `Ctrl-Z`.

Interface Config	From the Global Config mode, enter:
	`interface` slot/port or
	`interface loopback id` or
	`interface tunnel id`
	`interface` slot/port`(startrange)`-slot/port`(endrange)`
		To exit to the Global Config mode, enter `exit`. To return to the Privileged EXEC mode, enter `Ctrl-Z`.

Line Console	From the Global Config mode, enter `line console`.	To exit to the Global Config mode, enter `exit`. To return to the Privileged EXEC mode, enter `Ctrl-Z`.
AAA IAS User Config	From the Global Config mode, enter `aaa ias-user username name`.	To exit to the Global Config mode, enter `exit`. To return to the Privileged EXEC mode, enter `Ctrl-Z`.
Mail Server Config	From the Global Config mode, enter `mail-server address`	To exit to the Global Config mode, enter `exit`. To return to the Privileged EXEC mode, enter `Ctrl-Z`.

Table 6: CLI Mode Access and Exit (Cont.)

Command Mode	*Access Method*	*Exit or Access Previous Mode*
Policy-Map Config	From the Global Config mode, enter `policy-map`.	To exit to the Global Config mode, enter `exit`. To return to the Privileged EXEC mode, enter `Ctrl-Z`.
Policy-Class-Map Config	From the Policy Map mode enter `class`.	To exit to the Policy Map mode, enter `exit`. To return to the Privileged EXEC mode, enter `Ctrl-Z`.
Class-Map Config	From the Global Config mode, enter `class-map`, and specify the optional keyword `ipv4` to specify the Layer 3 protocol for this class. See "class-map" on page 798 for more information.	To exit to the Global Config mode, enter `exit`. To return to the Privileged EXEC mode, enter `Ctrl-Z`.
Ipv6-Class-Map Config	From the Global Config mode, enter `class-map` and specify the optional keyword `ipv6` to specify the Layer 3 protocol for this class. See "class-map" on page 798 for more information.	To exit to the Global Config mode, enter `exit`. To return to the Privileged EXEC mode, enter `Ctrl-Z`.
Router OSPF Config	From the Global Config mode, enter `router ospf`.	To exit to the Global Config mode, enter `exit`. To return to the Privileged EXEC mode, enter `Ctrl-Z`.
Router OSPFv3 Config	From the Global Config mode, enter `ipv6 router ospf`.	To exit to the Global Config mode, enter `exit`. To return to the Privileged EXEC mode, enter `Ctrl-Z`.
Router RIP Config	From the Global Config mode, enter `router rip`.	To exit to the Global Config mode, enter `exit`. To return to the Privileged EXEC mode, enter `Ctrl-Z`.
MAC Access-list Config	From the Global Config mode, enter `mac access-list extended name`.	To exit to the Global Config mode, enter `exit`. To return to the Privileged EXEC mode, enter `Ctrl-Z`.
TACACS Config	From the Global Config mode, enter `tacacs-server host ip-addr`, where `ip-addr` is the IP address of the TACACS server on your network.	To exit to the Global Config mode, enter `exit`. To return to the Privileged EXEC mode, enter `Ctrl-Z`.
DHCP Pool Config	From the Global Config mode, enter `ip dhcp pool pool-name`.	To exit to the Global Config mode, enter `exit`. To return to the Privileged EXEC mode, enter `Ctrl-Z`.
DHCPv6 Pool Config	From the Global Config mode, enter `ip dhcpv6 pool pool-name`.	To exit to the Global Config mode, enter `exit`. To return to the Privileged EXEC mode, enter `Ctrl-Z`.
Stack Global Config Mode	From the Global Config mode, enter the `stack` command.	To exit to the Global Config mode, enter the `exit` command. To return to the Privileged EXEC mode, enter `Ctrl-Z`.
ARP Access-List Config Mode	From the Global Config mode, enter the `arp access-list command`.	To exit to the Global Config mode, enter the `exit` command. To return to the Privileged EXEC mode, enter `Ctrl-Z`.
Wireless Config Mode	From the Global Config mode, enter `wireless`.	To exit to Global Config mode, enter `exit`. To return to User EXEC mode, enter `Ctrl-Z`.
AP Config Mode	From the Wireless Config mode, enter `ap database macaddr` where `macaddr` is the MAC address of the AP to configure.	To exit to Wireless Config mode, enter `exit`. To return to the User EXEC mode, enter `Ctrl-Z`.

Table 6: CLI Mode Access and Exit (Cont.)

Command Mode	*Access Method*	*Exit or Access Previous Mode*
AP Profile Config Mode	From the Wireless Config mode, enter `ap profile {1-16}` where `{1-16}` is the profile ID.	To exit to Wireless Config mode, enter `exit`. To return to User EXEC mode, enter `Ctrl-Z`.
AP Profile Radio Config Mode	From the AP Profile Config mode, enter `radio {1 | 2}`	To exit to AP Profile Config mode, enter `exit`. To return to User EXEC mode, enter `Ctrl-Z`.
AP Profile VAP Config Mode	From the AP Profile Radio Config mode, enter `vap {0-15}` where `{0-15}` is the VAP ID.	To exit to AP Profile Radio Configmode, enter `exit`. To return to User EXEC mode, enter `Ctrl-Z`.
Network Config Mode	From the Wireless Config mode, enter `network {1-64}` where `{1-64}` is the network ID.	To exit to Wireless Config mode, enter `exit`. To return to User EXEC mode, enter `Ctrl-Z`.
ARP Access-List Config Mode	From the Global Config mode, enter `arp access-list`	To exit to the Global Config mode, enter the `exit` command. To return to the Privileged EXEC mode, enter `Ctrl-Z`.
Captive Portal Config Mode	From the Global Config mode, enter `captive-portal`	To exit to the Global Config mode, enter the `exit` command. To return to the User EXEC mode, enter `Ctrl-Z`.
Captive Portal Instance Mode	From the Captive Portal Config mode, enter `configuration cp-id` where `cp-id` is the captive portal instance ID.	To exit to the Captive Portal Config mode, enter `exit`. To return to the User EXEC mode, enter `Ctrl-Z`.
WDS AP Group Config Mode	From Wireless Config mode, enter `wds-group {1-8}` where `{1-8}` is the group number.	To exit to the WDS AP Group Config mode, enter `exit`. To return to the User EXEC mode, enter `Ctrl-Z`.
Device Location Building Config Mode	From Wireless Config mode, enter `device-location building {1-8}` where `{1-8}` is the building number.	To exit to the Device Location Building Config mode, enter `exit`. To return to the User EXEC mode, enter `Ctrl-Z`.
Device Location Floor Config Mode	From the Device Location Building Config mode, enter `floor {1-20}` where `{1-20}` is the floor number.	To exit to the Device Location Floor Config mode, enter `exit`. To return to the User EXEC mode, enter `Ctrl-Z`.

Command Completion and Abbreviation

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

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

CLI Error Messages

If you enter a command and the system is unable to execute it, an error message appears. Table 7 describes the most common CLI error messages.

Table 7: 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 8 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 8: 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.

Table 8: CLI Editing Conventions (Cont.)

Key Sequence	*Description*
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 44.

Section 2: Stacking Commands

This chapter describes the stacking commands available in the DWS-4000 CLI.

Note: The stacking commands are available on the DWS-4000 Platform.

The Stacking Commands chapter includes the following sections:

Note: The commands in this section are in one of two functional groups:

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

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

Dedicated Port Stacking

This section describes the commands you use to configure dedicated port stacking.

stack

This command sets the mode to Stack Global Config.

Format	`stack`
Mode	Global Config

member

This command configures a switch. The *unit* is the switch identifier of the switch to be added/removed from the stack. The switchindex is the index into the database of the supported switch types, indicating the type of the switch being preconfigured. The switch index is a 32-bit integer. This command is executed on the Primary Management Unit.

Format member *unit switchindex*

Mode Stack Global Config

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

no member

This command removes a switch from the stack. The *unit* is the switch identifier of the switch to be removed from the stack. This command is executed on the Primary Management Unit.

Format no member *unit*

Mode Stack Global Config

switch priority

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

Default enabled

Format switch *unit* priority *value*

Mode Global Config

switch renumber

This command changes the switch identifier for a switch in the stack. The `oldunit` is the current switch identifier on the switch whose identifier is to be changed. The `newunit` is the updated value of the switch identifier. Upon execution, the switch will be configured with the configuration information for the new switch, if any. The old switch configuration information will be retained, however the old switch will be operationally unplugged. This command is executed on the Primary Management Unit.

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

Format `switch *oldunit* renumber *newunit*`

Mode Global Config

movemanagement

This command moves the Primary Management Unit functionality from one switch to another. The `fromunit` is the switch identifier on the current Primary Management Unit. The `tounit` is the switch identifier on the new Primary Management Unit. Upon execution, the entire stack (including all interfaces in the stack) is unconfigured and reconfigured with the configuration on the new Primary Management Unit. After the reload is complete, all stack management capability must be performed on the new Primary Management Unit. To preserve the current configuration across a stack move, execute the `copy system:running-config nvram:startup-config` (in Privileged EXEC) command before performing the stack move. A stack move causes all routes and layer 2 addresses to be lost. This command is executed on the Primary Management Unit. The system prompts you to confirm the management move.

Format `movemanagement *fromunit tounit*`

Mode Stack Global Config

standby

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

Note: The Standby Management Unit cannot be the current Management Unit. The Standby unit should be a management-capable unit.

Format `standby *unit number*`

Mode Stack Global Config

Parameter	*Description*
Standby Management Unit Number	Indicates the unit number which is to be the Standby Management Unit. **unit number** must be a valid unit number.

no standby

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

Format `no standby`

Mode Stack Global Config

slot

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

Format `slot` *unit/slot cardindex*

Mode Global Config

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

no slot

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

Format `no slot` *unit/slot cardindex*

Mode Global Config

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

set slot disable

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

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

Format `set slot disable [`*unit/slot*`] | all]`

Mode Global Config

no set slot disable

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

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

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

Mode Global Config

set slot power

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

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

Format `set slot power [unit/slot] | all]`

Mode Global Config

no set slot power

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

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

Format `no set slot power [unit/slot] | all]`

Mode Global Config

reload (Stack)

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

Format `reload [unit]`

Mode Global Config

show slot

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

Format `show slot [unit/slot]`

Mode User EXEC

Term	*Definition*
Slot	The slot identifier in a *unit/slot* format.
Slot Status	The slot is empty, full, or has encountered an error
Admin State	The slot administrative mode is enabled or disabled.
Power State	The slot power mode is enabled or disabled.
Configured Card Model Identifier	The model identifier of the card preconfigured in the slot. Model Identifier is a 32-character field used to identify a card.
Pluggable	Cards are pluggable or non-pluggable in the slot.
Power Down	Indicates whether the slot can be powered down.

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

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

show supported cardtype

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

Format `show supported cardtype [cardindex]`

Mode User EXEC

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

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

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

Term	*Definition*
Card Type	The 32-bit numeric card type for the supported card.
Model Identifier	The model identifier for the supported card type.
Card Description	The description for the supported card type.

show switch

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

Format `show switch [unit]`

Mode Privileged EXEC

Term	*Definition*
Switch	The unit identifier assigned to the switch.

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

Term	*Definition*
Management Status	Indicates whether the switch is the Primary Management Unit, a stack member, a configured standby switch, an operational standby switch, or the status is unassigned.
Preconfigured Model Identifier	The model identifier of a preconfigured switch ready to join the stack. The Model Identifier is a 32-character field assigned by the device manufacturer to identify the device.
Plugged-In Model Identifier	The model identifier of the switch in the stack. Model Identifier is a 32-character field assigned by the device manufacturer to identify the device.
Switch Status	The switch status. Possible values for this state are: OK, Unsupported, Code Mismatch, SDM Mismatch, Config Mismatch, or Not Present. A mismatch indicates that a stack unit is running a different version of the code, SDM template, or configuration than the management unit. If there is a Stacking Firmware Synchronization operation in progress status is shown as Updating Code.
Code Version	The detected version of code on this switch.

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

```
(Switching) #show switch

       Management   Standby      Preconfig      Plugged-in     Switch     Code
SW     Switch         Status         Model ID   Model ID       Status     Version
------ ------------ -------      ----------- ---------        -------    --------
1      Mgmt SW                   BCM-56224      BCM-56224      OK         M.3.22.1
2      Stack Mbr      Oper Stby  BCM-56224      BCM-56224      OK         M.3.22.1
```

When you specify a value for *unit*, the following information appears:

Term	*Definition*
Management Status	Indicates whether the switch is the Primary Management Unit, a stack member, or the status is unassigned.
Hardware Management Preference	The hardware management preference of the switch. The hardware management preference can be disabled or unassigned.
Admin Management Preference	The administrative management preference value assigned to the switch. This preference value indicates how likely the switch is to be chosen as the Primary Management Unit.
Switch Type	The 32-bit numeric switch type.
Model Identifier	The model identifier for this switch. Model Identifier is a 32-character field assigned by the device manufacturer to identify the device.
Switch Status	The switch status. Possible values are OK, Unsupported, Code Mismatch, Config Mismatch, SDM Mismatch, or Not Present.
Switch Description	The switch description.
Expected Code Type	The expected code type.
Expected Code Version	The expected code version.
Detected Code Version	The version of code running on this switch. If the switch is not present and the data is from pre-configuration, then the code version is None.
Detected Code in Flash	The version of code that is currently stored in FLASH memory on the switch. This code executes after the switch is reset. If the switch is not present and the data is from pre-configuration, then the code version is None.
SFS Last Attempt Status	The stack firmware synchronization status in the last attempt for the specified unit.
Serial Number	The serial number for the specified unit.
Up Time	The system up time.

show supported switchtype

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

Format `show supported switchtype [switchindex]`

Mode User EXEC
Privileged EXEC

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

Term	*Definition*
Switch Index (SID)	The index into the database of supported switch types. This index is used when preconfiguring a member to be added to the stack.
Model Identifier	The model identifier for the supported switch type.

Term	*Definition*
Management Preference	The management preference value of the switch type.
Code Version	The code load target identifier of the switch type.

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

Term	*Definition*
Switch Type	The 32-bit numeric switch type for the supported switch.
Model Identifier	The model identifier for the supported switch type.
Switch Description	The description for the supported switch type.

Stack Port Commands

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

stack-port

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

Default stack

Format `stack-port slot/port [{ethernet | stack}]`

Mode Stack Global Config

show stack-port

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

Format `show stack-port`

Mode Privileged EXEC

For Each Interface:

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

show stack-port counters

This command displays summary data counter information for all interfaces.

Format `show stack-port counters`

Mode Privileged EXEC

Term	*Definition*
Unit	The unit number.
Interface	The slot and port numbers.
Tx Data Rate	Trashing data rate in megabits per second on the stacking port.
Tx Error Rate	Platform-specific number of transmit errors per second.
Tx Total Errors	Platform-specific number of total transmit errors since power-up.
Rx Data Rate	Receive data rate in megabits per second on the stacking port.
Rx Error Rate	Platform-specific number of receive errors per second.
Rx Total Errors	Platform-specific number of total receive errors since power-up.

show stack-port diag

This command shows stack port diagnostics for each port and is only intended for Field Application Engineers (FAEs) and developers. An FAE will advise on the necessity to run this command and capture this information.

Format `show stack-port diag`

Mode Privileged EXEC

Term	*Definition*
Unit	The unit number.
Interface	The slot and port numbers.
Diagnostic Entry1	80 character string used for diagnostics.
Diagnostic Entry2	80 character string used for diagnostics.
Diagnostic Entry3	80 character string used for diagnostics.

Stack Firmware Synchronization Commands

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

boot auto-copy-sw

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

Default Disabled

Format `boot auto-copy-sw`

Mode Privileged Exec

no boot auto-copy-sw

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

Format `no boot auto-copy-sw`

Mode Privileged Exec

boot auto-copy-sw trap

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

Default Enabled

Format `boot auto-copy-sw trap`

Mode Privileged Exec

no boot auto-copy-sw trap

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

Format `no boot auto-copy-sw trap`

Mode Privileged Exec

boot auto-copy-sw allow-downgrade

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

Default Enabled

Format `boot auto-copy-sw allow-downgrade`

Mode Privileged Exec

no boot auto-copy-sw allow-downgrade

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

Format `no boot auto-copy-sw allow-downgrade`

Mode Privileged Exec

show auto-copy-sw

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

Format `show auto-copy-sw`

Mode Privileged Exec

Term	*Definition*
Synchronization	Shows whether the SFS feature is enabled.
SNMP Trap Status	Shows whether the stack will send traps for SFS events.
Allow Downgrade	Shows wether the manager is permitted to downgrade the firmware version of a stack member.

Nonstop Forwarding Commands

A switch can be described in terms of three semi-independent functions called the forwarding plane, the control plane, and the management plane. The forwarding plane forwards data packets. The forwarding plane is implemented in hardware. The control plane is the set of protocols that determine how the forwarding plane should forward packets, deciding which data packets are allowed to be forwarded and where they should go. Application software on the management unit acts as the control plane. The management plane is application software running on the management unit that provides interfaces allowing a network administrator to configure and monitor the device.

Nonstop forwarding (NSF) allows the forwarding plane of stack units to continue to forward packets while the control and management planes restart as a result of a power failure, hardware failure, or software fault on the management unit. A nonstop forwarding failover can also be manually initiated using the `initiate failover` command. Traffic flows that enter and exit the stack through physical ports on a unit other than the management continue with at most sub-second interruption when the management unit fails.

To prepare the backup management unit in case of a failover, applications on the management unit continuously checkpoint some state information to the backup unit. Changes to the running configuration are automatically copied to the backup unit. MAC addresses stay the same across a nonstop forwarding failover so that neighbors do not have to relearn them.

When a nonstop forwarding failover occurs, the control plane on the backup unit starts from a partially-initialized state and applies the checkpointed state information. While the control plane is initializing, the stack cannot react to external changes, such as network topology changes. Once the control plane is fully operational on the new management unit, the control plane ensures that the hardware state is updated as necessary. Control plane failover time depends on the size of the stack, the complexity of the configuration, and the speed of the CPU.

The management plane restarts when a failover occurs. Management connections must be reestablished.

For NSF to be effective, adjacent networking devices must not reroute traffic around the restarting device. DWS-4000 uses three techniques to prevent traffic from being rerouted:

1. A protocol may distribute a part of its control plane to stack units so that the protocol can give the appearance that it is still functional during the restart. Spanning tree and port channels use this technique.
2. A protocol may enlist the cooperation of its neighbors through a technique known as graceful restart. OSPF uses graceful restart if it is enabled (see “OSPF Graceful Restart Commands” on page 460 and “OSPF Graceful Restart Commands” on page 460).
3. A protocol may simply restart after the failover if neighbors react slowly enough that they will not normally detect the outage. The IP multicast routing protocols are a good example of this behavior.

To take full advantage of nonstop forwarding, layer 2 connections to neighbors should be via port channels that span two or more stack units, and layer 3 routes should be ECMP routes with next hops via physical ports on two or more units. The hardware can quickly move traffic flows from port channel members or ECMP paths on a failed unit to a surviving unit.

nsf (Stack Global Config Mode)

This command enables nonstop forwarding feature on the stack. When nonstop forwarding is enabled, if the management unit of a stack fails, the backup unit takes over as the master without clearing the hardware tables of any of the surviving units. Data traffic continues to be forwarded in hardware while the management functions initialize on the backup unit.

NSF is enabled by default on platforms that support it. The administrator may wish to disable NSF in order to redirect the CPU resources consumed by data checkpointing.

If a unit that does not support NSF is connected to the stack, then NSF is disabled on all stack members. When a unit that does not support NSF is disconnected from the stack and all other units support NSF, and NSF is administratively enabled, then NSF operation resumes.

Default enabled

Format `nsf`

Mode Stack Global Config Mode

no nsf

This command disables NSF on the stack.

Format `no nsf`

Mode Stack Global Config Mode

show nsf

This command displays global and per-unit information on NSF configuration on the stack.

Format `show nsf`

Mode Privileged Exec

Parameter	*Description*
NSF Administrative Status	Whether nonstop forwarding is administratively enabled or disabled. Default: Enabled
NSF Operational Status	Indicates whether NSF is enabled on the stack.

Parameter	*Description*
Last Startup Reason	The type of activation that caused the software to start the last time: • *Power-On* means that the switch rebooted. This could have been caused by a power cycle or an administrative `reload` command. • *Administrative Move* means that the administrator issued the `movemanagement` command for the stand-by manager to take over. • *Warm-Auto-Restart* means that the primary management card restarted due to a failure, and the system executed a nonstop forwarding failover. • *Cold-Auto-Restart* means that the system switched from the active manager to the backup manager and was unable to maintain user data traffic. This is usually caused by multiple failures occurring close together.
Time Since Last Restart	Time since the current management unit became the active management unit.
Restart in progress	Whether a restart is in progress.
Warm Restart Ready	Whether the system is ready to perform a nonstop forwarding failover from the management unit to the backup unit.
Copy of Running Configuration to Backup Unit: Status	Whether the running configuration on the backup unit includes all changes made on the management unit. Displays as Current or Stale.
Time Since Last Copy	When the running configuration was last copied from the management unit to the backup unit.
Time Until Next Copy	The number of seconds until the running configuration will be copied to the backup unit. This line only appears when the running configuration on the backup unit is Stale.
Per Unit Status Parameters	
NSF Support	Whether a unit supports NSF.

initiate failover

This command forces the backup unit to take over as the management unit and perform a *warm restart* of the stack. On a warm restart, the backup unit becomes the management unit without clearing its hardware tables (on a cold restart, hardware tables are cleared). Applications apply checkpointed data from the former management unit. The original management unit reboots.

If the system is not ready for a warm restart, for example because no backup unit has been elected or one or more members of the stack do not support nonstop forwarding, the command fails with a warning message.

The `movemanagement` command (see page 29) also transfers control from the current management unit; however, the hardware is cleared and all units reinitialize.

Format `initiate failover`

Mode Stack Global Config Mode

show checkpoint statistics

This command displays general information about the checkpoint service operation.

Format `show checkpoint statistics`

Mode Privileged Exec

Parameter	*Description*
Messages Checkpointed	Number of checkpoint messages transmitted to the backup unit. Range: Integer. Default: 0
Bytes Checkpointed	Number of bytes transmitted to the backup unit. Range: Integer. Default: 0
Time Since Counters Cleared	Number of days, hours, minutes and seconds since the counters were reset to zero. The counters are cleared when a unit becomes manager and with a support command. Range: Time Stamp. Default: 0d00:00:00
Checkpoint Message Rate	Average number of checkpoint messages per second. The average is computed over the time period since the counters were cleared. Range: Integer. Default: 0
Last 10-second Message Rate	Average number of checkpoint messages per second in the last 10-second interval. This average is updated once every 10 seconds. Range: Integer. Default: 0
Highest 10-second Message Rate	The highest rate recorded over a 10-second interval since the counters were cleared. Range: Integer. Default: 0

clear checkpoint statistics

This command clears all checkpoint statistics to their initial values.

Format `clear checkpoint statistics`

Mode Privileged Exec

Section 3: Management Commands

This chapter describes the management commands available in the DWS-4000 CLI.

The Management Commands chapter contains the following sections:

Note: The commands in this section are in one of three functional groups:

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

Network Interface Commands

This section describes the commands you use to configure a logical interface for management access. To configure the management VLAN, see "network mgmt_vlan" on page 234.

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. You can specify the `none` option to clear the IPv4 address and mask and the default gateway (i.e., reset each of these values to 0.0.0.0).

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

Mode Privileged EXEC

serviceport protocol

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

Format `serviceport protocol {none | bootp | dhcp}`

Mode Privileged EXEC

network parms

This command sets the IP address, subnet mask and gateway of the device. The IP address and the gateway must be on the same subnet. You can specify the none option to clear the IPv4 address and mask and the default gateway (i.e., to reset each of these values to 0.0.0.0).

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

Mode Privileged EXEC

network protocol

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

Default none

Format `network protocol {none | bootp | dhcp}`

Mode Privileged EXEC

network mac-address

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

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

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

Format `network mac-address` *`macaddr`*

Mode Privileged EXEC

network mac-type

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

Default burnedin

Format `network mac-type {local | burnedin}`

Mode Privileged EXEC

no network mac-type

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

Format `no network mac-type`

Mode Privileged EXEC

network javamode

This command specifies whether 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. The network interface is always considered to be up, whether or not any member ports are up; therefore, the `show network` command will always show the interface status as `Up`.

Format `show network`

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
Interface Status	The network interface status; it is always considered to be up.
IP Address	The IP address of the interface. The factory default value is 0.0.0.0.
Subnet Mask	The IP subnet mask for this interface. The factory default value is 0.0.0.0.
Default Gateway	The default gateway for this IP interface. The factory default value is 0.0.0.0.
IPv6 Administrative Mode	Whether enabled or disabled.
IPv6 Address/Length	The IPv6 address and length.
IPv6 Default Router	The IPv6 default router address.
Burned In MAC Address	The burned in MAC address used for in-band connectivity.

Term	*Definition*
Locally Administered MAC Address	If desired, a locally administered MAC address can be configured for in-band connectivity. To take effect, 'MAC Address Type' must be set to 'Locally Administered'. Enter the address as twelve hexadecimal digits (6 bytes) with a colon between each byte. Bit 1 of byte 0 must be set to a 1 and bit 0 to a 0, i.e. byte 0 should have the following mask 'xxxx xx10'. The MAC address used by this bridge when it must be referred to in a unique fashion. It is recommended that this be the numerically smallest MAC address of all ports that belong to this bridge. However it is only required to be unique. When concatenated with dot1dStpPriority a unique Bridge Identifier is formed which is used in the Spanning Tree Protocol.
MAC Address Type	The MAC address which should be used for in-band connectivity. The choices are the burned in or the Locally Administered address. The factory default is to use the burned in MAC address.
Configured IPv4 Protocol	The IPv4 network protocol being used. The options are bootp | dhcp | none.
Configured IPv6 Protocol	The IPv6 network protocol being used. The options are dhcp | none.
DHCPv6 Client DUID	The DHCPv6 client's unique client identifier. This row is displayed only when the configured IPv6 protocol is dhcp.
IPv6 Autoconfig Mode	Whether IPv6 Stateless address autoconfiguration is enabled or disabled.

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

```
(admin) #show network

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

show serviceport

This command displays service port configuration information.

Format `show serviceport`

Mode
- Privileged EXEC
- User EXEC

Term	*Definition*
Interface Status	The network interface status. It is always considered to be up.
IP Address	The IP address of the interface. The factory default value is 0.0.0.0.
Subnet Mask	The IP subnet mask for this interface. The factory default value is 0.0.0.0.
Default Gateway	The default gateway for this IP interface. The factory default value is 0.0.0.0.
IPv6 Administrative Mode	Whether enabled or disabled. Default value is enabled.
IPv6 Address/Length	The IPv6 address and length. Default is Link Local format.
IPv6 Default Router	TheIPv6 default router address on the service port. The factory default value is an unspecified address.
Configured IPv4 Protocol	The IPv4 network protocol being used. The options are bootp | dhcp | none.
Configured IPv6 Protocol	The IPv6 network protocol being used. The options are dhcp | none.
DHCPv6 Client DUID	The DHCPv6 client's unique client identifier. This row is displayed only when the configured IPv6 protocol is dhcp.
IPv6 Autoconfig Mode	Whether IPv6 Stateless address autoconfiguration is enabled or disabled.
Burned in MAC Address	The burned in MAC address used for in-band connectivity.

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

```
(admin) #show serviceport

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

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

line

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

Format `line {console | telnet | ssh}`

Mode Global Config

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

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

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

serial baudrate

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

Default 9600

Format `serial baudrate {1200 | 2400 | 4800 | 9600 | 19200 | 38400 | 57600 | 115200}`

Mode Line Config

no serial baudrate

This command sets the communication rate of the terminal interface.

Format `no serial baudrate`

Mode Line Config

serial timeout

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

Default 5

Format `serial timeout 0-160`

Mode Line Config

no serial timeout

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

Format `no serial timeout`

Mode Line Config

show serial

This command displays serial communication settings for the switch.

Format `show serial`

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
Serial Port Login Timeout (minutes)	The time, in minutes, of inactivity on a Serial port connection, after which the Switch will close the connection. 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.
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 or host name. Valid values for *port should* be a valid decimal integer in the range of 0 to 65535, where the default value is 23. If `[debug]` is used, the current Telnet options enabled is displayed. The optional *line* parameter sets the outbound Telnet operational mode as linemode where, by default, the operational mode is character mode. The `noecho` option disables local echo.

Format `telnet` *ip-address*|*hostname 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.

Default 5

Format `session-timeout` *`1–160`*

Mode Line Config

no session-timeout

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

Format `no session-timeout`

Mode Line Config

telnetcon maxsessions

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

Default 5

Format `telnetcon maxsessions` *`0–5`*

Mode Privileged EXEC

no telnetcon maxsessions

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

Format `no telnetcon maxsessions`

Mode Privileged EXEC

telnetcon timeout

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

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

Default 5

Format `telnetcon timeout` *`1–160`*

Mode Privileged EXEC

no telnetcon timeout

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

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

Format `no telnetcon timeout`

Mode Privileged EXEC

show telnet

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

Format `show telnet`

Modes
- Privileged EXEC
- User EXEC

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

show telnetcon

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

Format `show telnetcon`

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
Remote Connection Login Timeout (minutes)	This object indicates the number of minutes a remote connection session is allowed to remain inactive before being logged off. May be specified as a number from 1 to 160. The factory default is 5.
Maximum Number of Remote Connection Sessions	This object indicates the number of simultaneous remote connection sessions allowed. The factory default is 5.
Allow New Telnet Sessions	New Telnet sessions will not be allowed when this field is set to no. The factory default value is yes.

Secure Shell Commands

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

Note: The system allows a maximum of 5 SSH sessions.

ip ssh

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

Default disabled

Format `ip ssh`

Mode Privileged EXEC

ip ssh protocol

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

Default 1 and 2

Format `ip ssh protocol [1] [2]`

Mode Privileged EXEC

ip ssh server enable

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

Default 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

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

Management Security Commands

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

crypto certificate generate

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

Format `crypto certificate generate`

Mode Global Config

no crypto certificate generate

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

Format `no crypto certificate generate`

Mode Global Config

crypto key generate rsa

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

Format `crypto key generate rsa`

Mode Global Config

no crypto key generate rsa

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

Format `no crypto key generate rsa`

Mode Global Config

crypto key generate dsa

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

Format `crypto key generate dsa`

Mode Global Config

no crypto key generate dsa

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

Format `no crypto key generate dsa`

Mode Global Config

Hypertext Transfer Protocol Commands

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

ip http authentication

Use this command to specify authentication methods for http server users. The default configuration is the local user database is checked. This action has the same effect as the command `ip http authentication local`. The additional methods of authentication are used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify `none` as the final method in the command line. For example, if `none` is specified as an authentication method after `radius`, no authentication is used if the RADIUS server is down.

Default `local`

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

Mode Global Config

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

Example: The following example configures the http authentication.

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

no ip http authentication

Use this command to return to the default.

ip https authentication

Use this command to specify authentication methods for https server users. The default configuration is the local user database is checked. This action has the same effect as the command `ip https authentication local`. The additional methods of authentication are used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify `none` as the final method in the command line. For example, if `none` is specified as an authentication method after `radius`, no authentication is used if the RADIUS server is down.

Default `local`

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

Mode Global Config

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

Example: The following example configures https authentication.

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

no ip https authentication

Use this command to return to the default.

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 affected.

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

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 java

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

Default Enabled

Format `ip http java`

Mode Privileged EXEC

no ip http java

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

Format `no ip http java`

Mode Privileged EXEC

ip http session hard-timeout

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

Default 24

Format `ip http session hard-timeout` *`1–168`*

Mode Privileged EXEC

no ip http session hard-timeout

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

Format `no ip http session hard-timeout`

Mode Privileged EXEC

ip http session maxsessions

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

Default 16

Format `ip http session maxsessions 0–16`

Mode Privileged EXEC

no ip http session maxsessions

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

Format `no ip http session maxsessions`

Mode Privileged EXEC

ip http session soft-timeout

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

Default 5

Format `ip http session soft-timeout 1–60`

Mode Privileged EXEC

no ip http session soft-timeout

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

Format `no ip http session soft-timeout`

Mode Privileged EXEC

ip http secure-session hard-timeout

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

Default 24

Format `ip http secure-session hard-timeout 1–168`

Mode Privileged EXEC

no ip http secure-session hard-timeout

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

Format `no ip http secure-session hard-timeout`

Mode Privileged EXEC

ip http secure-session maxsessions

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

Default 16

Format `ip http secure-session maxsessions 0–16`

Mode Privileged EXEC

no ip http secure-session maxsessions

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

Format `no ip http secure-session maxsessions`

Mode Privileged EXEC

ip http secure-session soft-timeout

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

Default 5

Format `ip http secure-session soft-timeout 1–60`

Mode Privileged EXEC

no ip http secure-session soft-timeout

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

Format `no ip http secure-session soft-timeout`

Mode Privileged EXEC

ip http secure-port

This command 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

show ip http

This command displays the http settings for the switch.

Format `show ip http`

Mode Privileged EXEC

Term	*Definition*
HTTP Mode (Unsecure)	The unsecure HTTP server administrative mode.
Java Mode	The java applet administrative mode which applies to both secure and un-secure web connections.
Maximum Allowable HTTP Sessions	The number of allowable un-secure http sessions.
HTTP Session Hard Timeout	The hard timeout for un-secure http sessions in hours.
HTTP Session Soft Timeout	The soft timeout for un-secure http sessions in minutes.
HTTP Mode (Secure)	The secure HTTP server administrative mode.
Secure Port	The secure HTTP server port number.
Secure Protocol Level(s)	The protocol level may have the values of SSL3, TSL1, or both SSL3 and TSL1.
Maximum Allowable HTTPS Sessions	The number of allowable secure http sessions.
HTTPS Session Hard Timeout	The hard timeout for secure http sessions in hours.
HTTPS Session Soft Timeout	The soft timeout for secure http sessions in minutes.
Certificate Present	Indicates whether the secure-server certificate files are present on the device.
Certificate Generation in Progress	Indicates whether certificate generation is currently in progress.

Access Commands

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

disconnect

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

Format `disconnect {session_id | all}`

Mode Privileged EXEC

show loginsession

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

Format `show loginsession`

Mode Privileged EXEC

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

show loginsession long

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

Format `show loginsession long`

Mode Privileged EXEC

Example: The following shows an example of the command.

```
(switch) #show loginsession long
User Name
------------
admin
test1111test1111test1111test1111test1111test1111test1111test1111test1111
```

User Account Commands

This section describes the commands you use to add, manage, and delete system users. DWS-4000 software has two default users: admin and guest. The admin user can view and configure system settings, and the guest user can view settings.

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

aaa authentication login

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

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

Default
- `defaultList`. Used by the console and only contains the method none.
- `networkList`. Used by telnet and SSH and only contains the method local.

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

Mode Global Config

Parameter	*Definition*
default	Uses the listed authentication methods that follow this argument as the default list of methods when a user logs in.
list-name	Character string of up to 12 characters used to name the list of authentication methods activated when a user logs in.
method1... *[***method2...***]*	At least one from the following: • enable. Uses the enable password for authentication. • line. Uses the line password for authentication. • local. Uses the local username database for authentication. • none. Uses no authentication. • radius. Uses the list of all RADIUS servers for authentication. • tacacs. Uses the list of all TACACS servers for authentication.

Example: The following shows an example of the command.

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

no aaa authentication login

This command returns to the default.

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

Mode Global Config

aaa authentication enable

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

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

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

Note: Enable will not succeed for a level one user if no authentication method is defined. A level one user must authenticate to get to privileged EXEC mode. For example, if `none` is specified as an authentication method after radius, no authentication is used if the RADIUS server is down.

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

Default default

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

Mode Global Config

Parameter	*Description*
default	Uses the listed authentication methods that follow this argument as the default list of methods, when using higher privilege levels.
list-name	Character string used to name the list of authentication methods activated, when using access higher privilege levels. Range: 1–12 characters.
method1 *[***method2...***]*	Specify at least one from the following: • `enable`. Uses the enable password for authentication. • `line`. Uses the line password for authentication. • `none`. Uses no authentication. • `radius`. Uses the list of all RADIUS servers for authentication. • `tacacs`. Uses the list of all TACACS+ servers for authentication.

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

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

no aaa authentication enable

Use this command to return to the default configuration.

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

Mode Global Config

enable authentication

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

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

Mode Line Config

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

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

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

no enable authentication

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

Format `no enable authentication`

Mode Line Config

username

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

Format `username *name* passwd *password* [level *level*][encrypted][override-complexity-check]`

Mode Global Config

Parameter	*Description*
name	The name of the user. Range: 1–32 characters.
password	The authentication password for the user. Range 8–64 characters. This value can be zero if the `no passwords min-length` command has been executed. The special characters allowed in the password include ! # $ % & ' ( ) * + , - . / : ; < = > @ [\ ] ^ _ ` { | } ~.
level	The user level. Level 0 can be assigned by a level 15 user to another user to suspend that user's access. Range 0–15. Enter access level 1 for Read Access or 15 for Read/Write Access.
encrypted	Encrypted password entered, copied from another switch configuration.
override-complexity-check	Disables the validation of the password strength.

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

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

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

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

no username

Use this command to remove a user name.

username *name nopassword*

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

Format `username *name* nopassword *[level level]*`

Mode Global Config

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

username *name* unlock

Use this command to allows a locked user account to be unlocked. Only a user with read/write access can re-activate a locked user account.

Format `username *name* unlock`

Mode Global Config

username snmpv3 accessmode

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

Defaults
- admin - readwrite
- other - readonly

Format `username snmpv3 accessmode *username* {*readonly* | *readwrite*}`

Mode Global Config

no username snmpv3 accessmode

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

Format `no username snmpv3 accessmode *username*`

Mode Global Config

username snmpv3 authentication

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

Default no authentication

Format `username snmpv3 authentication` *`username`* {`none` | `md5` | `sha`}

Mode Global Config

no username snmpv3 authentication

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

Format `no username snmpv3 authentication` *`username`*

Mode Global Config

username snmpv3 encryption

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

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

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

Default no encryption

Format `username snmpv3 encryption` *`username`* {`none` | `des`*`[key]`*}

Mode Global Config

no username snmpv3 encryption

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

Format `no username snmpv3 encryption` *`username`*

Mode Global Config

username snmpv3 encryption encrypted

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

Default no encryption

Format `username snmpv3 encryption encrypted` *`username`* `des` *`key`*

Mode Global Config

show users

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

Format `show users`

Mode Privileged EXEC

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

show users long

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

Format `show users long`

Mode Privileged EXEC

Example: The following shows an example of the command.

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

show users accounts

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

Format `show users accounts [detail]`

Mode Privileged EXEC

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

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

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

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

```
(switch)#show users accounts

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

console#show users accounts detail

UserName..................................... admin
Privilege.................................... 15
Password Aging............................... ---
Password Expiry.............................. ---
Lockout...................................... False
Override Complexity Check.................... Disable
Password Strength............................ ---
```

show users login-history

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

Format `show users login-history [long]`

Mode Privileged EXEC

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

Example: The following example shows user login history outputs.

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

login authentication

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

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

Mode Line Configuration

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

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

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

no login authentication

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

passwd

This command allows the currently logged in user to change his or her password without having read/write privileges.

Format `password cr`

Mode User EXEC

password (Line Configuration)

Use this command to specify a password on a line. The default configuration is no password is specified.

Format `password password [encrypted]`

Mode Line Config

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

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

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

no password (Line Configuration)

Use this command to remove the password on a line.

password (User EXEC)

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

Format `password`

Mode User EXEC

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

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

enable passwd

This command prompts you to change the Privileged EXEC password. Passwords are a maximum of 64 alphanumeric characters. The password is case sensitive.

Format `enable passwd`

Mode Privileged EXEC

enable passwd encrypted

This command allows the administrator to transfer the enable password between devices without having to know the password. The *password* parameter must be exactly 128 hexadecimal characters.

Format `enable passwd encrypted password`

Mode Privileged EXEC

enable password

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

Format `enable password password [encrypted]`

Mode Privileged EXEC

Parameter	*Description*
password	Password for this level. Range: 8–64 characters.
encrypted	Encrypted password entered, copied from another switch configuration.

no enable password

Use this command to remove the password requirement.

passwords min-length

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

Default 8

Format `passwords min-length 8–64`

Mode Global Config

no passwords min-length

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

Format `no passwords min-length`

Mode Global Config

passwords history

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

Default 0

Format `passwords history` *`0–10`*

Mode Global Config

no passwords history

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

Format `no passwords history`

Mode Global Config

passwords aging

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

Default 0

Format `passwords aging` *`1–365`*

Mode Global Config

no passwords aging

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

Format `no passwords aging`

Mode Global Config

passwords lock-out

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

Default 0

Format `passwords lock-out 1–5`

Mode Global Config

no passwords lock-out

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

Format `no passwords lock-out`

Mode Global Config

passwords strength-check

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

Default Disable

Format `passwords strength-check`

Mode Global Config

no passwords aging

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

Format `no passwords strength-check`

Mode Global Config

passwords strength minimum uppercase-letters

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

Default 2

Format `passwords strength minimum uppercase-letters Length`

Mode Global Config

no passwords strength minimum uppercase-letters

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

Format `no passwords minimum uppercase-letter`

Mode Global Config

passwords strength minimum lowercase-letters

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

Default 2

Format `passwords strength minimum lowercase-letters` *Length*

Mode Global Config

no passwords strength minimum lowercase-letters

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

Format `no passwords minimum lowercase-letter`

Mode Global Config

passwords strength minimum numeric-characters

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

Default 2

Format `passwords strength minimum numeric-characters` *Length*

Mode Global Config

no passwords strength minimum numeric-characters

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

Format `no passwords minimum numeric-characters`

Mode Global Config

passwords strength minimum special-characters

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

Default 2

Format `passwords strength minimum special-characters` *Length*

Mode Global Config

no passwords strength minimum special-characters

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

Format `no passwords minimum special-characters`

Mode Global Config

passwords strength minimum consecutive-characters

Use this command to enforce a minimum number of consecutive characters that a password should contain. An example of consecutive characters is *abcd*. The valid range for *Length* is 0–16. If a password has consecutive characters more than the configured limit, it fails to configure. The default is 0. A minimum of 0 means no restriction on that set of characters.

Default 0

Format `passwords strength minimum consecutive-characters Length`

Mode Global Config

no passwords strength minimum consecutive-characters

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

Format `no passwords minimum consecutive-characters`

Mode Global Config

passwords strength minimum repeated-characters

Use this command to enforce a minimum number of repeated characters that a password should contain. An example of repeated characters is *aaaa*. The valid range for *Length* is 0–16. If a password has a repetition of characters more than the configured limit, it fails to configure. The default is 0. A minimum of 0 means no restriction on that set of characters.

Default 0

Format `passwords strength minimum repeated-characters Length`

Mode Global Config

no passwords strength minimum repeated-characters

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

Format `no passwords minimum repeated-characters`

Mode Global Config

passwords strength minimum character-classes

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

Default 4

Format `passwords strength minimum character-classes min`

Mode Global Config

no passwords strength minimum character-classes

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

Format `no passwords minimum character-classes`

Mode Global Config

passwords strength exclude-keyword

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

Format `passwords strength exclude-keyword keyword`

Mode Global Config

no passwords strength exclude-keyword

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

Format `no passwords exclude-keyword [keyword]`

Mode Global Config

show passwords configuration

Use this command to display the configured password management settings.

Format `show passwords configuration`

Mode Privileged EXEC

Term	*Definition*
Minimum Password Length	Minimum number of characters required when changing passwords.
Password History	Number of passwords to store for reuse prevention.
Password Aging	Length in days that a password is valid.
Lockout Attempts	Number of failed password login attempts before lockout.

Term	*Definition*
Minimum Password Uppercase Letters	Minimum number of uppercase characters required when configuring passwords.
Minimum Password Lowercase Letters	Minimum number of lowercase characters required when configuring passwords.
Minimum Password Numeric Characters	Minimum number of numeric characters required when configuring passwords.
Maximum Password Consecutive Characters	Maximum number of consecutive characters required that the password should contain when configuring passwords.
Maximum Password Repeated Characters	Maximum number of repetition of characters that the password should contain when configuring passwords.
Minimum Password Character Classes	Minimum number of character classes (uppercase, lowercase, numeric and special) required when configuring passwords.
Password Exclude-Keywords	The set of keywords to be excluded from the configured password when strength checking is enabled.

show passwords result

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

Format `show passwords result`

Mode Privileged EXEC

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

write memory

Use this command to save running configuration changes to NVRAM so that the changes you make will persist across a reboot. This command is the same as `copy system:running-config nvram:startup-config`.

Format `write memory`

Mode Privileged EXEC

aaa ias-user username

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

Use this command to add the specified user to the internal user database. This command also changes the mode to AAA User Config mode.

Format `aaa ias-user username user`

Mode Global Config

no aaa ias-user username

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

Format `no aaa ias-user username user`

Mode Global Config

password (AAA IAS User Configuration)

Use this command to specify a password for a user in the IAS database.

Format `password password [encrypted]`

Mode AAA IAS User Config

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

no password (AAA IAS User Configuration)

Use this command to remove the password for the user.

Format `password password [encrypted]`

Mode AAA IAS User Config

clear aaa ias-users

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

Format `clear aaa ias-users`

Mode Privileged Exec

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

show aaa ias-users

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

Format `show aaa ias-users`

Mode Privileged EXEC

SNMP Commands

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

snmp-server

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

Default none

Format `snmp-server {sysname name | location Loc | contact con}`

Mode Global Config

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

Format `snmp-server community ro` *name*

Mode Global Config

This command restricts access to switch information. The access mode is read-only (also called public).

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. This command can be used to configure a single interface or a range of interfaces.

Note: For other port security commands, see "Protected Ports Commands" on page 257.

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 linkmode

Note: This command may not be available on all platforms.

This command enables Link Up/Down traps for the entire switch. When enabled, link traps are sent only if the Link Trap flag setting associated with the port is enabled. See "snmp trap link-status" on page 90.

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 value for *ipaddr* or *ip6addr* can be an IPv4 address, IPv6 address, or hostname. The *snmpversion* is the version of SNMP. The version parameter options are snmpv1 or snmpv2. The SNMP trap address can be set using both an IPv4 address format as well as an IPv6 global address format.

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

```
(admin #) snmptrap mytrap ip6addr 3099::2
```

Note: The *name* parameter does not need to be unique, however; the *name* and receiver pair must be unique. Multiple entries can exist with the same *name*, as long as they are associated with a different receiver IP address or hostname. 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, "snmp-server community" on page 84.

Default	snmpv2
Format	`snmptrap` *name* {`ipaddr` | `ip6addr`} {*ipaddr* | *ip6addr* | *hostname*} [`snmpversion` *snmpversion*]
Mode	Global Config

no snmptrap

This command deletes trap receivers for a community.

Format	`no snmptrap` *name* {`ipaddr` | `ip6addr`} {*ipaddr* | *ip6addr* | *hostname*}
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* | *ip6addr* | *hostname*} *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 | hostnamenew}`

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 | ip6addr | hostname}`

Mode Global Config

no snmptrap mode

This command deactivates an SNMP trap. Disabled trap receivers are unable to receive traps.

Format `no snmptrap mode name {ipaddr | ip6addr | hostname}`

Mode Global Config

snmp trap link-status

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

Note: This command is valid only when the Link Up/Down Flag is enabled. See “snmp-server enable traps linkmode” on page 87.

Format `snmp trap link-status`

Mode Interface Config

no snmp trap link-status

This command disables link status traps by interface.

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

Format `no snmp trap link-status`

Mode Interface Config

snmp trap link-status all

This command enables link status traps for all interfaces.

Note: This command is valid only when the Link Up/Down Flag is enabled. See “snmp-server enable traps linkmode” on page 87.

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 87.

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

Term	*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

Term	*Definition*
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 IPv4 address to receive SNMP traps from this device.
IPv6 Address	The IPv6 address to receive SNMP traps from this device.
SNMP Version	SNMPv2
Status	The receiver's status (enabled or disabled).

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

```
(admin) #show snmptrap

SNMP Trap Name       IP Address       IPv6 Address     SNMP Version   Status
------------------- --------------- -------------------- ------------- ---------
Mytrap              2.2.2.2                               snmpv2        Enable
```

show trapflags

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

Format `show trapflags`

Mode Privileged EXEC

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

Term	*Definition*
ACL Traps	May be enabled or disabled. The factory default is disabled. Indicates whether ACL traps are sent.
BGP4 Traps	Can be enabled or disabled. The factory default is disabled. Indicates whether BGP4 traps are sent. (This field appears only on systems with the BGPv4 software package installed.)
DVMRP Traps	Can be enabled or disabled. The factory default is disabled. Indicates whether DVMRP traps are sent.
OSPFv2 Traps	Can be enabled or disabled. The factory default is disabled. Indicates whether OSPF traps are sent. If any of the OSPF trap flags are not enabled, then the command displays *disabled*. Otherwise, the command shows all the enabled OSPF traps' information.
OSPFv3 Traps	Can be enabled or disabled. The factory default is disabled. Indicates whether OSPF traps are sent. If any of the OSPFv3 trap flags are not enabled, then the command displays *disabled*. Otherwise, the command shows all the enabled OSPFv3 traps' information.
PIM Traps	Can be enabled or disabled. The factory default is disabled. Indicates whether PIM traps are sent.

RADIUS Commands

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

authorization network radius

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

Default disable

Format `authorization network radius`

Mode Global Config

no authorization network radius

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

Format `no authorization network radius`

Mode Global Config

radius accounting mode

This command is used to enable the RADIUS accounting function.

Default disabled

Format `radius accounting mode`

Mode Global Config

no radius accounting mode

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

Format `no radius accounting mode`

Mode Global Config

radius server attribute 4

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

Format `radius server attribute 4 [ipaddr]`

Mode Global Config

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

no radius server attribute 4

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

Format `no radius server attribute 4 [ipaddr]`

Mode Global Config

Example: The following shows an example of the command.

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

radius server host

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

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

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

Note: To 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|dnsname} [name servername] [port 0–65535]`

Mode Global Config

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

no radius server host

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

Format `no radius server host {auth | acct} {ipaddr|dnsname}`

Mode Global Config

Example: The following shows an example of the command.

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

radius server key

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

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

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

Format `radius server key {auth | acct} {ipaddr|dnsname} encrypted password`

Mode Global Config

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

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

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

radius server msgauth

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

Format `radius server msgauth ipaddr|dnsname`

Mode Global Config

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

no radius server msgauth

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

Format `no radius server msgauth ipaddr|dnsname`

Mode Global Config

radius server primary

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

Format `radius server primary {ipaddr|dnsname}`

Mode Global Config

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

radius server retransmit

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

Default 4

Format `radius server retransmit` *`retries`*

Mode Global Config

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

no radius server retransmit

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

Format `no radius server retransmit`

Mode Global Config

radius server timeout

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

Default 5

Format `radius server timeout` *`seconds`*

Mode Global Config

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

no radius server timeout

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

Format `no radius server timeout`

Mode Global Config

show radius

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

Format `show radius`

Mode Privileged EXEC

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

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

```
(Switch) #show radius

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

show radius servers

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

Format `show radius servers [{ipaddr|dnsname | name [servername]}]`

Mode Privileged EXEC

Field	*Description*
ipaddr	The IP address of the authenticating server.
dnsname	The DNS name of the authenticating server.
servername	The alias name to identify the server.
Current	The * symbol preceding the server host address specifies that the server is currently active.
Host Address	The IP address of the host.
Server Name	The name of the authenticating server.
Port	The port used for communication with the authenticating server.
Type	Specifies whether this server is a primary or secondary type.
Current Host Address	The IP address of the currently active authenticating server.
Secret Configured	Yes or No Boolean value that indicates whether this server is configured with a secret.
Number of Retransmits	The configured value of the maximum number of times a request packet is retransmitted.
Message Authenticator	A global parameter to indicate whether the Message Authenticator attribute is enabled or disabled.
Time Duration	The configured timeout value, in seconds, for request retransmissions.
RADIUS Accounting Mode	A global parameter to indicate whether the accounting mode for all the servers is enabled or not.
RADIUS Attribute 4 Mode	A global parameter to indicate whether the NAS-IP-Address attribute has been enabled to use in RADIUS requests.
RADIUS Attribute 4 Value	A global parameter that specifies the IP address to be used in NAS-IP-Address attribute used in RADIUS requests.

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

```
(Switch) #show radius servers

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

(Switch) #show radius servers name
```

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

(Switch) #show radius servers name Default_RADIUS_Server

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

(Switch) #show radius servers 192.168.37.58

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

show radius accounting

This command displays a summary of configured RADIUS accounting servers.

Format `show radius accounting name [servername]`

Mode Privileged EXEC

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

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

Term	*Definition*
Host Address	The IP address of the host.
Server Name	The name of the accounting server.
Port	The port used for communication with the accounting server.
Secret Configured	Yes or No Boolean value indicating whether this server is configured with a secret.

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

```
(Switch) #show radius accounting name

Host Address            Server Name                       Port     Secret
                                                                   Configured
---------------------- --------------------------------- -------- -----------
192.168.37.200          Network1_RADIUS_Server            1813     Yes
192.168.37.201          Network2_RADIUS_Server            1813     No
192.168.37.202          Network3_RADIUS_Server            1813     Yes
192.168.37.203          Network4_RADIUS_Server            1813     No


 (Switch) #show radius accounting name Default_RADIUS_Server

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

show radius accounting statistics

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

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

Mode Privileged EXEC

Term	*Definition*
ipaddr	The IP address of the server.
dnsname	The DNS name of the server.
servername	The alias name to identify the server.
RADIUS Accounting Server Name	The name of the accounting server.
Server Host Address	The IP address of the host.
Round Trip Time	The time interval, in hundredths of a second, between the most recent Accounting-Response and the Accounting-Request that matched it from this RADIUS accounting server.
Requests	The number of RADIUS Accounting-Request packets sent to this server. This number does not include retransmissions.

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

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

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

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

(Switch) #show radius accounting statistics name Default_RADIUS_Server

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

show radius statistics

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

Format `show radius statistics {ipaddr|dnsname | name servername}`

Mode Privileged EXEC

Term	*Definition*
ipaddr	The IP address of the server.
dnsname	The DNS name of the server.
servername	The alias name to identify the server.
RADIUS Server Name	The name of the authenticating server.
Server Host Address	The IP address of the host.
Access Requests	The number of RADIUS Access-Request packets sent to this server. This number does not include retransmissions.
Access Retransmissions	The number of RADIUS Access-Request packets retransmitted to this RADIUS authentication server.
Access Accepts	The number of RADIUS Access-Accept packets, including both valid and invalid packets, that were received from this server.
Access Rejects	The number of RADIUS Access-Reject packets, including both valid and invalid packets, that were received from this server.
Access Challenges	The number of RADIUS Access-Challenge packets, including both valid and invalid packets, that were received from this server.
Malformed Access Responses	The number of malformed RADIUS Access-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators or signature attributes or unknown types are not included as malformed access responses.
Bad Authenticators	The number of RADIUS Access-Response packets containing invalid authenticators or signature attributes received from this server.
Pending Requests	The number of RADIUS Access-Request packets destined for this server that have not yet timed out or received a response.
Timeouts	The number of authentication timeouts to this server.
Unknown Types	The number of packets of unknown type that were received from this server on the authentication port.
Packets Dropped	The number of RADIUS packets received from this server on the authentication port and dropped for some other reason.

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

```
(Switch) #show radius statistics 192.168.37.200

RADIUS Server Name..................... Default_RADIUS_Server
Server Host Address.................... 192.168.37.200
Access Requests........................ 0.00
Access Retransmissions................. 0
```

```
Access Accepts.............................. 0
Access Rejects.............................. 0
Access Challenges........................... 0
Malformed Access Responses.................. 0
Bad Authenticators.......................... 0
Pending Requests............................ 0
Timeouts.................................... 0
Unknown Types............................... 0
Packets Dropped............................. 0

(Switch) #show radius statistics name Default_RADIUS_Server

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

TACACS+ Commands

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

tacacs-server host

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

Format `tacacs-server host` *ip-address|hostname*

Mode Global Config

no tacacs-server host

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

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

Mode Global Config

tacacs-server key

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

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

Format `tacacs-server key [`*key-string* | `encrypted` *key-string*`]`

Mode Global Config

no tacacs-server key

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

Format `no tacacs-server key` *key-string*

Mode Global Config

tacacs-server 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).

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

Format `key [`*key-string* | `encrypted` *key-string*`]`

Mode TACACS Config

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|hostname]`*

Mode Privileged EXEC

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

Configuration Scripting Commands

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

Use the `show running-config` command (see "show running-config" on page 133) to capture the running configuration into a script. Use the `copy` command (see "copy" on page 152) 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:

- Script files are not distributed across the stack, and only live in the unit that is the master unit at the time of the file download.
- The file extension must be .scr.
- A maximum of ten scripts are allowed on the switch.
- The combined size of all script files on the switch shall not exceed 2048 KB.
- The maximum number of configuration file command lines is 2000.

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

The following lines show an example of a script:

```
! Script file for displaying management access

show telnet !Displays the information about remote connections

! Display information about direct connections

show serial

! End of the script file!
```

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

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

script apply

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

Format `script apply` *scriptname*

Mode Privileged EXEC

script delete

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

Format `script delete {`*scriptname* `| all}`

Mode Privileged EXEC

script list

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

Format `script list`

Mode Global Config

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

script show

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

Format `script show` *scriptname*

Mode Privileged EXEC

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

script validate

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

Format `script validate` *scriptname*

Mode Privileged EXEC

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

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

copy (pre-login banner)

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

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

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

set prompt

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

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

hostname

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

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

TR-069 Client Commands

TR-069 is a bidirectional remote management specification for customer premises equipment (CPE). TR-069 defines the CPE WAN Management Protocol (CWMP), which enables communication between the CPE and an auto-configuration server (ACS) to perform auto-configuration, dynamic service provisioning, software/ firmware image management, status and performance monitoring, and diagnostics.

These commands configure the switch as a TR-069 client CPE.

tr069 acs

This command configures the ACS parameters used by the CPE to initiate a session with the ACS.

Default
- URL = no value
- user = 000AF7-Broadcom
- password = burned-in MAC Address of the CPE
- upgrades managed = false

Format `tr069 acs {url acs-address | user string | password string | upgrades managed}`

Mode Global Config

Parameter	*Description*
url	The IP address of the ACS.
user	The user name for logging into the ACS server. Up to 256 characters.
password	The password for logging in to the ACS server. Up to 256 characters.
upgrades managed	If this parameter is included, then image upgrades will be handled by TR-069 communication with the ACS. In this case, the CPE cannot use the CLI, Web, or SNMP interfaces for upgrades. If this command is not included, then the ACL will not manage upgrades and the user interfaces will be available for this purpose.

no tr069 acs

This command clears the specified ACS parameters.

Format `no tr069 acs {url acs-address | user string | password string | upgrades managed}`

Mode Global Config

tr069 periodic inform

This command configures the periodic inform messages that the CPE sends to the ACS. The inform messages initiate a set of transactions and communicate CPE limitations. These parameters define when and how frequently the CPE sends inform messages to the ACS.

Default
- mode = disable
- interval = 0
- time = zero value (0000-00-00T00:00:00)

Format `tr069 periodic inform {mode | interval 1–2592000 | time time-string}`

Mode Global Config

Parameter	*Description*
mode	Sets Periodic Inform Mode to enable or disable. When enabled, the CPE will send periodic inform messages to the ACS.
interval	The duration in seconds of the interval for which the CPE attempts to connect with the ACS when Periodic Inform mode is enabled. Periodic informs are not sent if this interval is set to 0. The range is 1–2592000 seconds.
time	The time when the CPE should initiate the Inform calls to the ACS. Each Inform call must occur at this reference time plus or minus an integer multiple of the Periodic Inform Interval. The time should be entered in format *yyyy-mm-ddThh:mm:ss*. A zero value (000-00-00T00:00:00) indicates that no particular time reference is specified. That is, the CPE chooses the time reference but adheres to the specified Periodic Inform Interval.

tr069 connection-request

A TR-069 session can be initiated by the CPE, or the ACS can connect to the CPE to instruct it to request a session. This command configures the parameters against which the ACS is authenticated when the ACS connects to the CPE.

Default
- user = 000AF7-Broadcom
- password = burned-in MAC Address of the CPE

Format `tr069 connection-request {user string | password string}`

Mode Global Config

Parameter	*Description*
user	The user name for authenticating an ACS connections to the CPE. Up to 256 characters.
password	The password for authenticating an ACS connections to the CPE. Up to 256 characters.

no tr069 connection-request

This command returns the specified connection request parameters to their default values.

Format `no tr069 connection-request {user | password | url | upgrades-managed}`

Mode Global Config

show tr069

This show command displays the configured tr-069 client parameters and statistics.

Format `show tr069 {summary | statistics}`

Mode Privileged EXEC

The following output items are shown by this command:

Term	*Definition*
ACS URL	URL for the CPE to connect to the ACS using the CPE WAN Management Protocol.
ACS User	User name for authenticating the CPE when it makes a TR-069 connection to the ACS. This parameter is used only when SSL support is not present.
Periodic Inform Mode	Indicates whether or not the CPE sends CPE information to the ACS using Periodic Inform Messages.
Periodic Inform Interval	The duration in seconds of the interval in which the CPE attempts to connect with the ACS when Periodic Inform mode is enabled.
Periodic Inform Time	The time when the CPE should initiate the inform messages. Each inform message must occur at this reference time plus or minus an integer multiple of the Periodic Inform Interval. A zero value (0000 0000T00:00:00) Indicates that no particular time reference is specified. That is, the CPE chooses the time reference but adheres to the specified Periodic Inform Interval.
Upgrades Managed	Indicates whether or not the ACS will manage upgrades for the CPE. If True, the CPE cannot use the user interfaces (CLI, Web, and SNMP) for upgrades. If False, the CPE can use these interfaces to perform software upgrades.
Connection Request User	User name for authenticating an ACS when it makes a connection request to the CPE.
Connection Request URL	User HTTP URL for an ACS to make a connection request notification to the CPE.
Parameter Key	Provides a means to track the last successful transaction done by ACS.
ACS CA Certificate Loaded	Specifies whether the ACS certification authority is successfully loaded or not.
Client Certificate Loaded	Specifies whether the CPE client authentication certificate is successfully loaded or not.
Client Private Key Loaded	Specifies whether the CPE client private key is successfully loaded or not.
Total Inform Messages Sent	Number of inform messages sent by the CPE since the last system reset.
Total Connection Requests Received	Number of connection request messages received by the CPE since the last system reset.
Total Faults	Number of faults encountered by the CPE since the last system reset.
Method Not-Supported Faults	Number of RPC requests with an unsupported RPC method received by the CPE since the last system reset.
Request Denied Faults	Number of RPC requests denied by the CPE since the last system reset.
Internal Errors	Number of RPC requests failed due to internal processing errors by the CPE since the last system reset.
Invalid Argument Faults	Number of RPC methods with invalid arguments received by the CPE since the last system reset.

Term	*Definition*
Resources Exceeded Faults	Number of errors occurred due to unavailability of resources at the CPE since the last system reset.
Invalid Parameter Name Faults	Number of RPC methods with invalid parameter names received by the CPE since the last system reset.
Invalid Parameter Type Faults	Number of RPC methods with invalid parameter names received by the CPE since the last system reset.
Invalid Parameter Value Faults	Number of RPC methods with invalid parameter values received by the CPE since the last system reset.
Invalid Write Attempt Faults	Number of attempts to set a non writable parameter by the CPE since the last system reset.
Notification Request Rejections	Number of SetParameterAttributes RPC methods denied by the CPE since the last system reset.
Download Failures	Number of download failures encountered by the CPE since the last system reset.
Upload Failures	Number of upload failures encountered by the CPE since the last system reset.
File Transfer Server Authentication Failures	Number of file server authentication failures encountered by the CPE since the last system reset.
Vendor Default Faults	Number of vendor-defined errors encountered by the CPE since the last system reset.

Section 4: Utility Commands

This chapter describes the utility commands available in the DWS-4000 CLI.

The Utility Commands chapter includes the following sections:

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

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

AutoInstall Commands

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

AutoInstall includes the following support:

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

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

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

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

boot autoinstall

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

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

boot host retrycount

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

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

no boot host retrycount

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

Format `no boot host retrycount`

Mode Privileged EXEC

boot host dhcp

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

Default disabled

Format `boot host dhcp`

Mode Privileged EXEC

no boot host dhcp

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

Format `no boot host dhcp`

Mode Privileged EXEC

boot host autosave

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

Default disabled

Format `boot host autosave`

Mode Privileged EXEC

no boot host autosave

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

Format `no boot host autosave`

Mode Privileged EXEC

boot host autoreboot

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

Default enabled

Format `boot host autoreboot`

Mode Privileged EXEC

no boot host autoreboot

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

Format `no boot host autoreboot`

Mode Privileged EXEC

erase startup-config

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

Format `erase startup-config`

Mode Privileged EXEC

show autoinstall

This command displays the current status of the AutoInstall process.

Format `show autoinstall`

Mode Privileged EXEC

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

```
(switch) #show autoinstall

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

Dual Image Commands

DWS-4000 software supports a dual image feature that allows the switch to have two software images in the permanent storage. You can specify which image is the active image to be loaded in subsequent reboots. This feature allows reduced down-time when you upgrade or downgrade the software.

delete

This command deletes the backup image file from the permanent storage. The optional *unit* parameter is valid only on Stacks. Error will be returned, if this parameter is provided, on Standalone systems. In a stack, the *unit* parameter identifies the node on which this command must be executed. When this parameter is not supplied, the command is executed on all nodes in a Stack.

Format `delete [unit] backup`

Mode Privileged EXEC

boot system

This command activates the specified image. It will be the active-image for subsequent reboots and will be loaded by the boot loader. The current active-image is marked as the backup-image for subsequent reboots. If the specified image doesn't exist on the system, this command returns an error message. The optional *unit* parameter is valid only in Stacking, where the *unit* parameter identifies the node on which this command must be executed. When this parameter is not supplied, the command is executed on all nodes in a Stack.

Format `boot system [unit] {active | backup}`

Mode Privileged EXEC

show bootvar

This command displays the version information and the activation status for the current active and backup images on the supplied unit (node) of the Stack. If you do not specify a unit number, the command displays image details for all nodes on the Stack. The command also displays any text description associated with an image. This command, when used on a Standalone system, displays the switch activation status. For a standalone system, the unit parameter is not valid.

Format `show bootvar [unit]`

Mode Privileged EXEC

filedescr

This command associates a given text description with an image. Any existing description will be replaced. The command is executed on all nodes in a Stack.

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

Mode Privileged EXEC

update bootcode

This command updates the bootcode (boot loader) on the switch. The bootcode is read from the active-image for subsequent reboots.The optional *unit* parameter is valid only on Stacks. Error will be returned, if this parameter is provided, on Standalone systems. For Stacking, the *unit* parameter identifies the node on which this command must be executed. When this parameter is not supplied, the command is executed on all nodes in a Stack.

Format `update bootcode [unit]`

Mode Privileged EXEC

System Information and Statistics Commands

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

show arp switch

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

Format `show arp switch`

Mode Privileged EXEC

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

show eventlog

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

Format `show eventlog [unit]`

Mode Privileged EXEC

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

Note: Event log information is retained across a switch 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 command "show version" on page 123.

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

Term	*Definition*
System Description	Text used to identify the product name of this switch.
Machine Type	The machine model as defined by the Vital Product Data.
Machine Model	The machine model as defined by the Vital Product Data
Serial Number	The unique box serial number for this switch.
FRU Number	The field replaceable unit number.
Part Number	Manufacturing part number.
Maintenance Level	Hardware changes that are significant to software.
Manufacturer	Manufacturer descriptor field.
Burned in MAC Address	Universally assigned network address.
Software Version	The release.version.revision number of the code currently running on the switch.
Operating System	The operating system currently running on the switch.
Network Processing Device	The type of the processor microcode.
Additional Packages	The additional packages incorporated into this system.

show interface

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

Format `show interface {slot/port | switchport}`

Mode Privileged EXEC

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

Parameters	*Definition*
Packets Received Without Error	The total number of packets (including broadcast packets and multicast packets) received by the processor.
Packets Received With Error	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Broadcast Packets Received	The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.
Packets Transmitted Without Error	The total number of packets transmitted out of the interface.
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` are as follows:

Term	*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.

Term	*Definition*
Packets Received	• **Total Packets Received (Octets)** - The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including Frame Check Sequence (FCS) octets). This object can be used as a reasonable estimate of Ethernet utilization. If greater precision is desired, the etherStatsPkts and etherStatsOctets objects should be sampled before and after a common interval. The result of this equation is the value Utilization which is the percent utilization of the Ethernet segment on a scale of 0 to 100 percent. • **Packets Received 64 Octets** - The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets). • **Packets Received 65–127 Octets** - The total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets). • **Packets Received 128–255 Octets** - The total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets). • **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** - The total number of packets (including bad packets) received and transmitted that were 64 octets in length (excluding framing bits but including FCS octets). • **Packets RX and TX 65–127 Octets** - The total number of packets (including bad packets) received and transmitted that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets). • **Packets RX and TX 128–255 Octets** - The total number of packets (including bad packets) received and transmitted that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets). • **Packets RX and TX 256–511 Octets** - The total number of packets (including bad packets) received and transmitted that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).

Term	*Definition*
Packets Received (con't)	• **Packets RX and TX 512–1023 Octets** - The total number of packets (including bad packets) received and transmitted that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets). • **Packets RX and TX 1024–1518 Octets** - The total number of packets (including bad packets) received and transmitted that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets). • **Packets RX and TX 1519–1522 Octets** - The total number of packets (including bad packets) received and transmitted that were between 1519 and 1522 octets in length inclusive (excluding framing bits but including FCS octets). • **Packets RX and TX 1523–2047 Octets** - The total number of packets received and transmitted that were between 1523 and 2047 octets in length inclusive (excluding framing bits, but including FCS octets) and were otherwise well formed. • **Packets RX and TX 2048–4095 Octets** - The total number of packets received that were between 2048 and 4095 octets in length inclusive (excluding framing bits, but including FCS octets) and were otherwise well formed. • **Packets RX and TX 4096–9216 Octets** - The total number of packets received that were between 4096 and 9216 octets in length inclusive (excluding framing bits, but including FCS octets) and were otherwise well formed.
Packets Received Successfully	• **Total Packets Received Without Error** - The total number of packets received that were without errors. • **Unicast Packets Received** - The number of subnetwork-unicast packets delivered to a higher-layer protocol. • **Multicast Packets Received** - The total number of good packets received that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address. • **Broadcast Packets Received** - The total number of good packets received that were directed to the broadcast address. Note that this does not include multicast packets.
Packets Received with MAC Errors	• **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.

Term	*Definition*
Received Packets Not Forwarded	• **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. • **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.
Packets Transmitted Octets	• **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). • **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.

Term	*Definition*
Packets Transmitted Successfully	• **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.
Transmit Errors	• **Total Errors** - The sum of Single, Multiple, and Excessive Collisions. • **Tx FCS Errors** - The total number of packets transmitted that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with an integral number of octets. • **Oversized** - The total number of frames that exceeded the max permitted frame size. This counter has a max increment rate of 815 counts per sec. at 10 Mb/s. • **Underrun Errors** - The total number of frames discarded because the transmit FIFO buffer became empty during frame transmission.
Transmit Discards	• **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.

Term	*Definition*
Protocol Statistics	• **802.3x Pause Frames Transmitted** - A count of MAC Control frames transmitted on this interface with an opcode indicating the PAUSE operation. This counter does not increment when the interface is operating in half-duplex mode. • **GVRP PDUs Received** - The count of GVRP PDUs received in the GARP layer. • **GVRP PDUs Transmitted** - The count of GVRP PDUs transmitted from the GARP layer. • **GVRP Failed Registrations** - The number of times attempted GVRP registrations could not be completed. • **GMRP PDUs Received** - The count of GMRP PDUs received in the GARP layer. • **GMRP PDUs Transmitted** - The count of GMRP PDUs transmitted from the GARP layer. • **GMRP Failed Registrations** - The number of times attempted GMRP registrations could not be completed. • **STP BPDUs Transmitted** - Spanning Tree Protocol Bridge Protocol Data Units sent. • **STP BPDUs Received** - Spanning Tree Protocol Bridge Protocol Data Units received. • **RST BPDUs Transmitted** - Rapid Spanning Tree Protocol Bridge Protocol Data Units sent. • **RSTP BPDUs Received** - Rapid Spanning Tree Protocol Bridge Protocol Data Units received. • **MSTP BPDUs Transmitted** - Multiple Spanning Tree Protocol Bridge Protocol Data Units sent. • **MSTP BPDUs Received** - Multiple Spanning Tree Protocol Bridge Protocol Data Units received.
Dot1x Statistics	• **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.

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

Term	*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.

Term	*Definition*
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.
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. These entries are used by the transparent bridging function to determine how to forward a received frame.

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

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

Mode Privileged EXEC

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

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

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

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

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

show process cpu

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

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

Note: This command is available in VxWorks and Linux 2.6 only.

Format show process cpu

Mode Privileged EXEC

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

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

 CPU Utilization:

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

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

```
(Switching) #show process cpu

Memory Utilization Report
status      bytes
------ ----------
  free  192980480
alloc   53409968
Task Utilization Report
Task                    Utilization
----------------------- -----------
```

```
bcmL2X.0                    0.75%
bcmCNTR.0                   0.20%
bcmLINK.0                   0.35%
DHCP snoop                  0.10%
Dynamic ARP Inspection      0.10%
dot1s_timer_task            0.10%
dhcpsPingTask               0.20%
```

show running-config

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

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

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

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

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

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

- If all the flags are enabled, then the command displays `trapflags all`.
- If all the flags in a particular group are enabled, then the command displays `trapflags` *`group_name`* `all`.
- If some, but not all, of the flags in that group are enabled, the command displays `trapflags` *`groupname flag-name`*.

Format `show running-config [all | scriptname]`

Mode Privileged EXEC

show sysinfo

This command displays switch information.

Format `show sysinfo`

Mode Privileged EXEC

Term	*Definition*
Switch Description	Text used to identify this switch.
System Name	Name used to identify the switch.The factory default is blank. To configure the system name, see “snmp-server” on page 84.
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 84.
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 84.
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 isdp neighbors
- show logging
- show event log
- show logging buffered
- show trap log
- show running config

Format `show tech-support`

Mode Privileged EXEC

terminal length

Use this command to set the number of lines of output to be displayed on the screen, i.e. pagination, for the `show running-config` and `show running-config all` commands. The terminal length size is either zero or a number in the range of 5 to 48. After the user-configured number of lines is displayed in one page, the system prompts the user for `--More-- or (q)uit.` Press q or Q to quit, or press any key to display the next set of 5–48 lines. The command terminal length 0 disables pagination and, as a result, the output of the show running-config command is displayed immediately.

Default 24 lines per page

Format `terminal length 0|5–48`

Mode Privileged EXEC

no terminal length

Use this command to set the terminal length to the default value.

show terminal length

Use this command to display the value of the user-configured terminal length size.

Format `show terminal length`

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 cli-command

This command enables the CLI command logging feature, which enables the DWS-4000 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

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|hostname* is the IP address of the logging host. The *addresstype* indicates the type of address IPv4 or IPv6 or DNS being passed. 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|hostname} addresstype [port][severitylevel]`

Mode Global Config

logging host remove

This command disables logging to host. See "show logging hosts" on page 139 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

Term	*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

Term	*Definition*
Buffered (In-Memory) Logging	Shows whether the In-Memory log is enabled or disabled.
Buffered Logging Wrapping Behavior	The behavior of the In Memory log when faced with a log full situation.
Buffered Log Count	The count of valid entries in the buffered log.

show logging hosts

This command displays all configured logging hosts. The *unit* is the switch identifier and has a range of 1–8.

Format `show logging hosts` *unit*

Mode Privileged EXEC

Term	*Definition*
Host Index	(Used for deleting hosts.)
IP Address / Hostname	IP address or hostname of the logging host.
Severity Level	The minimum severity to log to the specified address. The possible values are emergency (0), alert (1), critical (2), error (3), warning (4), notice (5), info (6), or debug (7).
Port	The server port number, which is the port on the local host from which syslog messages are sent.
Host Status	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

Term	*Definition*
Number of Traps Since Last Reset	The number of traps since the last boot.
Trap Log Capacity	The number of traps the system can retain.
Number of Traps Since Log Last Viewed	The number of new traps since the command was last executed.
Log	The log number.
System Time Up	How long the system had been running at the time the trap was sent.
Trap	The text of the trap message.

Email Alerting and Mail Server Commands

logging email

This command enables email alerting and sets the lowest severity level for which log messages are emailed. If you specify a severity level, log messages at or above this severity level, but below the urgent severity level, are emailed in a non-urgent manner by collecting them together until the log time expires. You can specify the *severitylevel* value as either an integer from 0 to 7 or symbolically through one of the following keywords: `emergency (0), alert (1), critical (2), error (3), warning (4), notice (5), info (6), or debug (7).`

Default disabled; when enabled, log messages at or above severity Warning (4) are emailed

Format `logging email [severitylevel]`

Mode Global Config

no logging email

This command disables email alerting.

Format `no logging email`

Mode Global Config

logging email urgent

This command sets the lowest severity level at which log messages are emailed immediately in a single email message. Specify the *severitylevel* value as either an integer from 0 to 7 or symbolically through one of the following keywords: *emergency (0), alert (1), critical (2), error (3), warning (4), notice (5), info (6), or debug (7)*. Specify none to indicate that log messages are collected and sent in a batch email at a specified interval.

Default Alert (1) and emergency (0) messages are sent immediately.

Format `logging email urgent {severitylevel | none}`

Mode Global Config

no logging email urgent

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

Format `no logging email urgent`

Mode Global Config

logging email message-type to-addr

This command configures the email address to which messages are sent. The message types supported are `urgent`, `non-urgent`, and `both`. For each supported severity level, multiple email addresses can be configured. The *to-email-addr* variable is a standard email address, for example admin@yourcompany.com.

Format `logging email message-type {urgent |non-urgent |both} to-addr to-email-addr`

Mode Global Config

no logging email message-type to-addr

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

Format `no logging email message-type {urgent |non-urgent |both} to-addr to-email-addr`

Mode Global Config

logging email from-addr

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

Default switch@broadcom.com

Format `logging email from-addr from-email-addr`

Mode Global Config

no logging email from-addr

This command removes the configured email source address.

Format `no logging email from-addr` *`from-email-addr`*

Mode Global Config

logging email message-type subject

This command configures the subject line of the email for the specified type.

Default For urgent messages: Urgent Log Messages
For non-urgent messages: Non Urgent Log Messages

Format `logging email message-type {urgent |non-urgent |both} subject` *`subject`*

Mode Global Config

no logging email message-type subject

This command removes the configured email subject for the specified message type and restores it to the default email subject.

Format `no logging email message-type {urgent |non-urgent |both} subject`

Mode Global Config

logging email logtime

This command configures how frequently non-urgent email messages are sent. Non-urgent messages are collected and sent in a batch email at the specified interval. The valid range is every 30–1440 minutes.

Default 30 minutes

Format `logging email logtime` *`minutes`*

Mode Global Config

no logging email logtime

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

Format `no logging email logtime`

Mode Global Config

logging traps

This command sets the severity at which SNMP traps are logged and sent in an email. Specify the *severitylevel* value as either an integer from 0 to 7 or symbolically through one of the following keywords: emergency (0), alert (1), critical (2), error (3), warning (4), notice (5), info (6), or debug (7).

Default Info (6) messages and higher are logged.

Format `logging traps severitylevel`

Mode Global Config

no logging traps

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

Format `no logging traps`

Mode Global Config

logging email test message-type

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

Format `logging email test message-type {urgent |non-urgent |both} message-body message-body`

Mode Global Config

show logging email config

This command displays information about the email alert configuration.

Format `show logging email config`

Mode Privileged EXEC

Term	*Definition*
Email Alert Logging	The administrative status of the feature: enabled or disabled
Email Alert From Address	The email address of the sender (the switch).
Email Alert Urgent Severity Level	The lowest severity level that is considered urgent. Messages of this type are sent immediately.
Email Alert Non Urgent Severity Level	The lowest severity level that is considered non-urgent. Messages of this type, up to the urgent level, are collected and sent in a batch email. Log messages that are less severe are not sent in an email message at all.
Email Alert Trap Severity Level	The lowest severity level at which traps are logged.
Email Alert Notification Period	The amount of time to wait between non-urgent messages.
Email Alert To Address Table	The configured email recipients.

Term	*Definition*
Email Alert Subject Table	The subject lines included in urgent (Type 1) and non-urgent (Type 2) messages.
For Msg Type urgent, subject is	The configured email subject for sending urgent messages.
For Msg Type non-urgent, subject is	The configured email subject for sending non-urgent messages.

show logging email statistics

This command displays email alerting statistics.

Format `show logging email statistics`

Mode Privileged EXEC

Term	*Definition*
Email Alert Operation Status	The operational status of the email alerting feature.
No of Email Failures	The number of email messages that have attempted to be sent but were unsuccessful.
No of Email Sent	The number of email messages that were sent from the switch since the counter was cleared.
Time Since Last Email Sent	The amount of time that has passed since the last email was sent from the switch.

clear logging email statistics

This command resets the email alerting statistics.

Format `clear logging email statistics`

Mode Privileged EXEC

mail-server

This command configures the SMTP server to which the switch sends email alert messages and changes the mode to Mail Server Configuration mode. The server address can be in the IPv4, IPv6, or DNS name format.

Format `mail-server {ip-address | ipv6-address | hostname}`

Mode Global Config

no mail-server

This command removes the specified SMTP server from the configuration.

Format `no mail-server {ip-address | ipv6-address | hostname}`

Mode Global Config

security

This command sets the email alerting security protocol by enabling the switch to use TLS authentication with the SMTP Server. If the TLS mode is enabled on the switch but the SMTP sever does not support TLS mode, no email is sent to the SMTP server.

Default none

Format `security {tlsv1 | none}`

Mode Mail Server Config

port

This command configures the TCP port to use for communication with the SMTP server. The recommended port for TLSv1 is 465, and for no security (i.e. none) it is 25. However, any nonstandard port in the range 1 to 65535 is also allowed.

Default 25

Format `port {465 | 25 | 1–65535}`

Mode Mail Server Config

username

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

Default admin

Format `username name`

Mode Mail Server Config

password

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

Default admin

Format `password password`

Mode Mail Server Config

show mail-server config

This command displays information about the email alert configuration.

Format `show mail-server {ip-address | hostname | all} config`

Mode Privileged EXEC

Term	*Definition*
No of mail servers configured	The number of SMTP servers configured on the switch.
Email Alert Mail Server Address	The IPv4/IPv6 address or DNS hostname of the configured SMTP server.
Email Alert Mail Server Port	The TCP port the switch uses to send email to the SMTP server
Email Alert Security Protocol	The security protocol (TLS or none) the switch uses to authenticate with the SMTP server.
Email Alert Username	The username the switch uses to authenticate with the SMTP server.
Email Alert Password	The password the switch uses to authenticate with the SMTP server.

System Utility and Clear Commands

This section describes the commands you use to help troubleshoot connectivity issues and to restore various configurations to their factory defaults.

traceroute

Use the `traceroute` command to discover the routes that packets actually take when traveling to their destination through the network on a hop-by-hop basis. Traceroute continues to provide a synchronous response when initiated from the CLI.

Default

- count: 3 probes
- interval: 3 seconds
- size: 0 bytes
- port: 33434
- maxTtl: 30 hops
- maxFail: 5 probes
- initTtl: 1 hop
-

Format `traceroute {`*`ipaddr`*`|`*`hostname`*`} [initTtl `*`initTtl`*`] [maxTtl `*`maxTtl`*`] [maxFail `*`maxFail`*`] [interval `*`interval`*`] [count `*`count`*`] [port `*`port`*`] [size `*`size`*`]`

Mode Privileged EXEC

Using the options described below, you can specify the initial and maximum time-to-live (TTL) in probe packets, the maximum number of failures before termination, the number of probes sent for each TTL, and the size of each probe.

Parameter	*Description*
ipaddr/hostname	The *ipaddr* value should be a valid IP address. The *hostname* value should be a valid hostname.
initTtl	Use `initTtl` to specify the initial time-to-live (TTL), the maximum number of router hops between the local and remote system. Range is 0 to 255.
maxTtl	Use `maxTtle` to specify the maximum TTL. Range is 1 to 255.
maxFail	Use `maxFail` to terminate the traceroute after failing to receive a response for this number of consecutive probes. Range is 0 to 255.
interval	If a response is not received within this interval, then traceroute considers that probe a failure (printing *) and sends the next probe. If traceroute does receive a response to a probe within this interval, then it sends the next probe immediately. Range is 1 to 60 seconds.
count	Use the optional `count` parameter to specify the number of probes to send for each TTL value. Range is 1 to 10 probes.
port	Use the optional `port` parameter to specify destination UDP port of the probe. This should be an unused port on the remote destination system. Range is 1 to 65535.
size	Use the optional `size` parameter to specify the size, in bytes, of the payload of the Echo Requests sent. Range is 0 to 65507 bytes.

The following are examples of the CLI command.

Example: traceroute Success:

```
(Routing) # traceroute 10.240.10.115 initTtl 1 maxTtl 4 maxFail 0 interval 1 count 3 port 33434 size
43
 Traceroute to 10.240.10.115 ,4 hops max 43 byte packets:
1 10.240.4.1   708 msec     41 msec     11 msec
2 10.240.10.115   0 msec     0 msec     0 msec

Hop Count = 1 Last TTL = 2 Test attempt = 6 Test Success = 6
```

Example: traceroute Failure:

```
(Routing) # traceroute 10.40.1.1 initTtl 1 maxFail 0 interval 1 count 3
port 33434 size 43
Traceroute to 10.40.1.1 ,30 hops max 43 byte packets:
1 10.240.4.1   19 msec     18 msec     9 msec
2 10.240.1.252   0 msec     0 msec     1 msec
3 172.31.0.9   277 msec     276 msec     277 msec
4 10.254.1.1   289 msec     327 msec     282 msec
5 10.254.21.2   287 msec     293 msec     296 msec
6 192.168.76.2   290 msec     291 msec     289 msec
7 0.0.0.0   0 msec *
Hop Count = 6 Last TTL = 7 Test attempt = 19 Test Success = 18
```

traceroute ipv6

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 {*ipv6-address* | *hostname*} parameter must be a valid IPv6 address or hostname. 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 zero (0) to 65535. The default value is 33434.

Default	port: 33434
Format	`traceroute ipv6 {`*ipv6-address*	*hostname*`} [port` *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 current configuration on the switch to the default values. It does not reset the switch.

Format	`clear config`
Mode	Privileged EXEC

clear counters

This command clears the statistics for a specified slot/port, for all the ports, or for the entire switch based upon the argument.

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

logout

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

Note: Save configuration changes before logging out.

Format `logout`

Modes
- Privileged EXEC
- User EXEC

ping

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

Default
- The default count is 1.
- The default interval is 3 seconds.
- The default size is 0 bytes.

Format `ping {`*`ipaddress`* | *`hostname`*`}[count `*`count`*`] [interval `*`interval`*`] [size `*`size`*`]`

Modes
- Privileged EXEC
- User EXEC

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

Parameter	*Description*
count	Use the `count` parameter to specify the number of ping packets (ICMP Echo requests) that are sent to the destination address specified by the *`ip-address`* field. The range for *`count`* is 1 to 15 requests.
interval	Use the `interval` parameter to specify the time between Echo Requests, in seconds. Range is 1 to 60 seconds.
size	Use the `size` parameter to specify the size, in bytes, of the payload of the Echo Requests sent. Range is 0 to 65507 bytes.

The following are examples of the CLI command.

Example: ping success:

```
(Routing) #ping 10.254.2.160 count 3 interval 1 size 255
Pinging 10.254.2.160 with 255 bytes of data:

Received response for icmp_seq = 0. time = 275268 usec
Received response for icmp_seq = 1. time = 274009 usec
Received response for icmp_seq = 2. time = 279459 usec

----10.254.2.160 PING statistics----
3 packets transmitted, 3 packets received, 0% packet loss
round-trip (msec) min/avg/max = 274/279/276
```

Example: ping failure:

In Case of Unreachable Destination:

```
(Routing) # ping 192.168.254.222 count 3 interval 1 size 255
Pinging 192.168.254.222 with 255 bytes of data:
Received Response: Unreachable Destination
Received Response :Unreachable Destination
Received Response :Unreachable Destination
----192.168.254.222  PING statistics----
3 packets transmitted,3 packets received, 0% packet loss
round-trip (msec) min/avg/max = 0/0/0
```

In Case Of Request TimedOut:

```
(Routing) # ping 1.1.1.1 count 1 interval 3
Pinging 1.1.1.1 with 0 bytes of data:

----1.1.1.1 PING statistics----
1 packets transmitted,0 packets received, 100% packet loss
round-trip (msec) min/avg/max = 0/0/0
```

quit

This command closes the current telnet connection or resets the current serial connection. The system asks you whether to save configuration changes before quitting.

Format `quit`

Modes
- Privileged EXEC
- User EXEC

reload

This command resets the switch without powering it off. Reset means that all network connections are terminated and the boot code executes. The switch uses the stored configuration to initialize the switch. You are prompted to confirm that the reset should proceed. The LEDs on the switch indicate a successful reset.

Format `reload`

Mode Privileged EXEC

copy

The copy command uploads and downloads files to and from the switch. You can also use the copy command to manage the dual images (active and backup) on the file system. Upload and download files from a server by using TFTP or Xmodem. SFTP and SCP are available as additional transfer methods if the software package supports secure management.

Format copy *source destination*

Mode Privileged EXEC

Replace the *source* and *destination* parameters with the options in Table 9 on page 152. For the *url* source or destination, use one of the following values:
{xmodem | tftp://*ipaddr*|*hostname* | *ip6address*|*hostname/filepath/filename* [noval]| sftp|scp://*username@ipaddr* | *ipv6address/filepath/filename*}

Note: The maximum length for the file path is 160 characters, and the maximum length for the file name is 32 characters.

For TFTP, SFTP and SCP, the *ipaddr*|*hostname* parameter is the IP address or host name of the server, *filepath* is the path to the file, and *filename* is the name of the file you want to upload or download. For SFTP and SCP, the *username* parameter is the username for logging into the remote server via SSH.

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

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

Table 9: Copy Parameters

Source	*Destination*	*Description*
nvram:backup-config	nvram:startup-config	Copies the backup configuration to the startup configuration.
nvram:clibanner	*url*	Copies the CLI banner to a server.
nvram:errorlog	*url*	Copies the error log file to a server.
nvram:fastpath.cfg	*url*	Uploads the binary config 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	nvram:backup-config	Copies the startup configuration to the backup configuration.
nvram:startup-config	*url*	Copies the startup configuration to a server.
nvram:traplog	*url*	Copies the trap log file to a server.

Table 9: Copy Parameters (Cont.)

Source	*Destination*	*Description*
system:running-config	nvram:startup-config	Saves the running configuration to nvram.
url	nvram:clibanner	Downloads the CLI banner to the system.
url	nvram:fastpath.cfg	Downloads the binary config file to the system.
url	nvram:script *destfilename*	Downloads a configuration script file to the system. During the download of a configuration script, the copy command validates the script. In case of any error, the command lists all the lines at the end of the validation process and prompts you to confirm before copying the script file.
url	nvram:script *destfilename* noval	When you use this option, the copy command will not validate the downloaded script file. An example of the CLI command follows:
(Routing) #copy tftp://1.1.1.1/file.scr nvram:script file.scr noval		
url	nvram:sshkey-dsa	Downloads an SSH key file. For more information, see "Secure Shell Commands" on page 55.
url	nvram:sshkey-rsa1	Downloads an SSH key file.
url	nvram:sshkey-rsa2	Downloads an SSH key file.
url	nvram:sslpem-dhweak	Downloads an HTTP secure-server certificate.
url	nvram:sslpem-dhstrong	Downloads an HTTP secure-server certificate.
url	nvram:sslpem-root	Downloads an HTTP secure-server certificate. For more information, see "Hypertext Transfer Protocol Commands" on page 59.
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	kernel	Downloads a code file to the system.
url	ias-users	Downloads an IAS users database file to the system. When the IAS users file is downloaded, the switch IAS user's database is replaced with the users and their attributes available in the downloaded file.
url	{active | backup}	Download an image from the remote server to either image. In a stacking environment, the downloaded image is distributed to the stack nodes.
{active | backup}	*url*	Upload either image to the remote server.
active	backup	Copy the active image to the backup image.
backup	active	Copy the backup image to the active image.
{active | backup}	unit://*unit*/{active | backup}	Copy an image from the management node to a given node in a Stack. Use the unit parameter to specify the node to which the image should be copied.
{active | backup}	unit://*/{active | backup}	Copy an image from the management node to all of the nodes in a Stack.

Keying for Advanced Features

This section describes the commands you use to enter the licence key to access advanced features. You cannot access the advanced features without a valid license key.

license advanced

This command enables a particular feature. This command also enables the corresponding show commands for a feature.

Note: If the feature is enabled, the feature is visible in the output of the `show running-config` command. The *`key`* parameter specifies the hexadecimal key for the feature.

Default none

Format `license advanced` *`key`*

Mode Privileged EXEC

no license advanced

This command disables a particular feature. This command also disables the corresponding show commands. The *`key`* parameter specifies the hexadecimal key for the feature.

Format `no license advanced` *`key`*

Mode Privileged EXEC

show key-features

This command displays the enabled or disabled status for all keyable features.

Format `show key-features`

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
Function	This is the name of the keyable component or feature.
Status	Enabled or disabled.

Simple Network Time Protocol Commands

This section describes the commands you use to automatically configure the system time and date by using Simple Network Time Protocol (SNTP).

sntp broadcast client poll-interval

This command sets the poll interval for SNTP broadcast clients in seconds as a power of two where *poll-interval* can be a value from 6 to 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. The default value is 0, which means that the SNTP port is not configured by the user. In the default case, the actual client port value used in SNTP packets is assigned by the underlying OS.

Default 0

Format `sntp client port portid`

Mode Global Config

no sntp client port

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

Format `no sntp client port`

Mode Global Config

sntp unicast client poll-interval

This command sets the poll interval for SNTP unicast clients in seconds as a power of two where *poll-interval* can be a value from 6 to 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 server address can be either an IPv4 address or an IPv6 address. The optional priority can be a value of 1–3, the version a value of 1–4, and the port id a value of 1–65535.

Format `sntp server {ipaddress | ipv6address | hostname} [priority [version [portid]]]`

Mode Global Config

no sntp server

This command deletes an server from the configured SNTP servers.

Format `no sntp server remove {ipaddress | ipv6address | hostname}`

Mode Global Config

show sntp

This command is used to display SNTP settings and status.

Format `show sntp`

Mode Privileged EXEC

Term	*Definition*
Last Update Time	Time of last clock update.
Last Attempt Time	Time of last transmit query (in unicast mode).
Last Attempt Status	Status of the last SNTP request (in unicast mode) or unsolicited message (in broadcast mode).
Broadcast Count	Current number of unsolicited broadcast messages that have been received and processed by the SNTP client since last reboot.
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

Term	*Definition*
Client Supported Modes	Supported SNTP Modes (Broadcast, Unicast, or Multicast).
SNTP Version	The highest SNTP version the client supports.
Port	SNTP Client Port. The field displays the value 0 if it is default value. When the client port value is 0, if the client is in broadcast mode, it binds to port 123; if the client is in unicast mode, it binds to the port assigned by the underlying OS.
Client Mode	Configured SNTP Client Mode.

show sntp server

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

Format `show sntp server`

Mode Privileged EXEC

Term	*Definition*
Server IP Address / Hostname	IP address or hostname of configured SNTP Server.
Server Type	Address type of server (IPv4, IPv6, or DNS).
Server Stratum	Claimed stratum of the server for the last received valid packet.
Server Reference ID	Reference clock identifier of the server for the last received valid packet.
Server Mode	SNTP Server mode.
Server Maximum Entries	Total number of SNTP Servers allowed.
Server Current Entries	Total number of SNTP configured.

For each configured server:

Term	*Definition*
IP Address / Hostname	IP address or hostname of configured SNTP Server.
Address Type	Address Type of configured SNTP server (IPv4, IPv6, or DNS).
Priority	IP priority type of the configured server.
Version	SNTP Version number of the server. The protocol version used to query the server in unicast mode.
Port	Server Port Number.
Last Attempt Time	Last server attempt time for the specified server.
Last Update Status	Last server attempt status for the server.
Total Unicast Requests	Number of requests to the server.
Failed Unicast Requests	Number of failed requests from server.

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 23. *Minutes* is an integer from 0 to 59.

Default 1 (day)

Format `lease [{days [hours] [minutes] | infinite}]`

Mode DHCP Pool Config

no lease

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

Format `no lease`

Mode DHCP Pool Config

network (DHCP Pool Config)

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

Default none

Format `network networknumber [{mask | prefixlength}]`

Mode DHCP Pool Config

no network

This command removes the subnet number and mask.

Format `no network`

Mode DHCP Pool Config

bootfile

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

Format `bootfile filename`

Mode DHCP Pool Config

no bootfile

This command deletes the boot image name.

Format `no bootfile`

Mode DHCP Pool Config

domain-name

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

Default none

Format `domain-name domain`

Mode DHCP Pool Config

no domain-name

This command removes the domain name.

Format `no domain-name`

Mode DHCP Pool Config

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:

- 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 restores the number of ping packets to the default value.

Format `no ip dhcp ping packets`

Mode Global Config

service dhcp

This command enables the DHCP server.

Default disabled

Format `service dhcp`

Mode Global Config

no service dhcp

This command disables the DHCP server.

Format `no service dhcp`

Mode Global Config

ip dhcp bootp automatic

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

Default disabled

Format `ip dhcp bootp automatic`

Mode Global Config

no ip dhcp bootp automatic

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

Format `no ip dhcp bootp automatic`

Mode Global Config

ip dhcp conflict logging

This command enables conflict logging on 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.

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

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

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

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

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

The following additional field is displayed for Dynamic pool type:

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

The following additional fields are displayed for Manual pool type:

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

show ip dhcp server statistics

This command displays DHCP server statistics.

Format `show ip dhcp server statistics`

Modes
- Privileged EXEC
- User EXEC

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

Message Received:

Message	*Definition*
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.

Message Sent:

Message	*Definition*
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

Term	*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.

DNS Client Commands

These commands are used in the Domain Name System (DNS), an Internet directory service. DNS is how domain names are translated into IP addresses. When enabled, the DNS client provides a hostname lookup service to other components of DWS-4000.

ip domain lookup

Use this command to enable the DNS client.

Default enabled

Format `ip domain lookup`

Mode Global Config

no ip domain lookup

Use this command to disable the DNS client.

Format `no ip domain lookup`

Mode Global Config

ip domain name

Use this command to define a default domain name that DWS-4000 software uses to complete unqualified host names (names with a domain name). By default, no default domain name is configured in the system. *name* may not be longer than 255 characters and should not include an initial period. This *name* should be used only when the default domain name list, configured using the `ip domain list command,` is empty.

Default none

Format `ip domain name` *name*

Mode Global Config

Example: The CLI command `ip domain name yahoo.com` will configure yahoo.com as a default domain name. For an unqualified hostname xxx, a DNS query is made to find the IP address corresponding to xxx.yahoo.com.

no ip domain name

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

Format `no ip domain name`

Mode Global Config

ip domain list

Use this command to define a list of default domain names to complete unqualified names. By default, the list is empty. Each name must be no more than 256 characters, and should not include an initial period. The default domain name, configured using the `ip domain name` command, is used only when the default domain name list is empty. A maximum of 32 names can be entered in to this list.

Default none

Format `ip domain list` *name*

Mode Global Config

no ip domain list

Use this command to delete a name from a list.

Format `no ip domain list` *name*

Mode Global Config

ip name server

Use this command to configure the available name servers. Up to eight servers can be defined in one command or by using multiple commands. The parameter *server-address* is a valid IPv4 or IPv6 address of the server. The preference of the servers is determined by the order they were entered.

Format `ip name-server` *server-address1* [*server-address2...server-address8*]

Mode Global Config

no ip name server

Use this command to remove a name server.

Format `no ip name-server [server-address1...server-address8]`

Mode Global Config

ip host

Use this command to define static host name-to-address mapping in the host cache. The parameter *name* is host name and *ip address* is the IP address of the host. The hostname can include 1–158 alphanumeric characters, periods, hyphens, underscores, and non-consecutive spaces. Hostnames that include one or more space must be enclosed in quotation marks, for example “lab-pc 45”.

Default none

Format `ip host name ipaddress`

Mode Global Config

no ip host

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

Format `no ip host name`

Mode Global Config

ipv6 host

Use this command to define static host name-to-IPv6 address mapping in the host cache. The parameter *name* is host name and *v6 address* is the IPv6 address of the host. The hostname can include 1–158 alphanumeric characters, periods, hyphens, and spaces. Hostnames that include one or more space must be enclosed in quotation marks, for example “lab-pc 45”.

Default none

Format `ipv6 host name v6 address`

Mode Global Config

no ipv6 host

Use this command to remove the static host name-to-IPv6 address mapping in the host cache.

Format `no ipv6 host name`

Mode Global Config

ip domain retry

Use this command to specify the number of times to retry sending Domain Name System (DNS) queries. The parameter *number* indicates the number of times to retry sending a DNS query to the DNS server. This number ranges from 0 to 100.

Default 2

Format `ip domain retry number`

Mode Global Config

no ip domain retry

Use this command to return to the default.

Format `no ip domain retry number`

Mode Global Config

ip domain timeout

Use this command to specify the amount of time to wait for a response to a DNS query. The parameter *seconds* specifies the time, in seconds, to wait for a response to a DNS query. The parameter *seconds* ranges from 0 to 3600.

Default 3

Format `ip domain timeout seconds`

Mode Global Config

no ip domain timeout

Use this command to return to the default setting.

Format `no ip domain timeout seconds`

Mode Global Config

clear host

Use this command to delete entries from the host name-to-address cache. This command clears the entries from the DNS cache maintained by the software. This command clears both IPv4 and IPv6 entries.

Format `clear host {name | all}`

Mode Privileged EXEC

Field	*Description*
name	A particular host entry to remove. The parameter *name* ranges from 1–255 characters.
all	Removes all entries.

show hosts

Use this command to display the default domain name, a list of name server hosts, the static and the cached list of host names and addresses. The parameter *name* ranges from 1–255 characters. This command displays both IPv4 and IPv6 entries.

Format `show hosts [name]`

Mode User EXEC

Field	*Description*
Host Name	Domain host name.
Default Domain	Default domain name.
Default Domain List	Default domain list.
Domain Name Lookup	DNS client enabled/disabled.
Number of Retries	Number of time to retry sending Domain Name System (DNS) queries.
Retry Timeout Period	Amount of time to wait for a response to a DNS query.
Name Servers	Configured name servers.

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

```
<SWITCHING> show hosts

Host name..................... Device
Default domain................ gm.com
Default domain list........... yahoo.com, Stanford.edu, rediff.com
Domain Name lookup............ Enabled
Number of retries............. 5
Retry timeout period.......... 1500
Name servers (Preference order)... 176.16.1.18 176.16.1.19
Configured host name-to-address mapping:

Host                          Addresses
----------------------------- -----------------------------
accounting.gm.com             176.16.8.8

Host              Total    Elapsed       Type       Addresses
--------------- -------- ------    --------     --------------
www.stanford.edu   72        3          IP         171.64.14.203
```

IP Address Conflict Commands

The commands in this section help troubleshoot IP address conflicts.

ip address-conflict-detect run

This command triggers the switch to run active address conflict detection by sending gratuitous ARP packets for IPv4 addresses on the switch.

Format `ip address-conflict-detect run`

Mode Global Config

show ip address-conflict

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

Format `show ip address-conflict`

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
Address Conflict Detection Status	Identifies whether the switch has detected an address conflict on any IP address.
Last Conflicting IP Address	The IP Address that was last detected as conflicting on any interface.
Last Conflicting MAC Address	The MAC Address of the conflicting host that was last detected on any interface.
Time Since Conflict Detected	The time in days, hours, minutes and seconds since the last address conflict was detected.

clear ip address-conflict

This command clears the detected address conflict status information.

Format `clear ip address-conflict`

Modes
- Privileged EXEC
- User EXEC

Serviceability Packet Tracing Commands

These commands improve the capability of network engineers to diagnose conditions affecting their DWS-4000 product.

Caution! The output of `debug` commands can be long and may adversely affect system performance.

debug arp

Use this command to enable ARP debug protocol messages.

Default disabled

Format `debug arp`

Mode Privileged EXEC

no debug arp

Use this command to disable ARP debug protocol messages.

Format `no debug arp`

Mode Privileged EXEC

debug auto-voip

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

Default disabled

Format `debug auto-voip [H323|SCCP|SIP]`

Mode Privileged EXEC

no debug auto-voip

Use this command to disable Auto VOIP debug messages.

Format `no debug auto-voip`

Mode Privileged EXEC

debug bgp packet

Use this command to enable BGP packet debug trace.

Default disabled

Format `debug bgp`

Mode Privileged EXEC

no debug bgp

Use this command to disable BGP debug messages.

Format `no debug bgp`

Mode Privileged EXEC

debug clear

This command disables all previously enabled debug traces.

Default disabled

Format `debug clear`

Mode Privileged EXEC

debug console

This command enables the display of `debug` trace output on the login session in which it is executed. Debug console display must be enabled in order to view any trace output. The output of debug trace commands will appear on all login sessions for which debug console has been enabled. The configuration of this command remains in effect for the life of the login session. The effect of this command is not persistent across resets.

Default disabled

Format `debug console`

Mode Privileged EXEC

no debug console

This command disables the display of debug trace output on the login session in which it is executed.

Format `no debug console`

Mode Privileged EXEC

debug dhcp packet

This command displays debug information about DHCPv4 client activities and traces DHCPv4 packets to and from the local DHCPv4 client.

Default disabled

Format `debug dhcp packet [transmit | receive]`

Mode Privileged EXEC

no debug dhcp

This command disables the display of debug trace output for DHCPv4 client activity.

Format `no debug dhcp packet [transmit | receive]`

Mode Privileged EXEC

debug dot1x packet

Use this command to enable dot1x packet debug trace.

Default disabled

Format `debug dot1x`

Mode Privileged EXEC

no debug dot1x packet

Use this command to disable dot1x packet debug trace.

Format `no debug dot1x`

Mode Privileged EXEC

debug igmpsnooping packet

This command enables tracing of IGMP Snooping packets received and transmitted by the switch.

Default disabled

Format `debug igmpsnooping packet`

Mode Privileged EXEC

no debug igmpsnooping packet

This command disables tracing of IGMP Snooping packets.

Format `no debug igmpsnooping packet`

Mode Privileged EXEC

debug igmpsnooping packet transmit

This command enables tracing of IGMP Snooping packets transmitted by the switch. Snooping should be enabled on the device and the interface in order to monitor packets for a particular interface.

Default disabled

Format `debug igmpsnooping packet transmit`

Mode Privileged EXEC

A sample output of the trace message is shown below.

```
<15> JAN 01 02:45:06 192.168.17.29-1 IGMPSNOOP[185429992]: igmp_snooping_debug.c(116) 908 % Pkt TX
- Intf: 1/0/20(20), Vlan_Id:1 Src_Mac: 00:03:0e:00:00:00 Dest_Mac: 01:00:5e:00:00:01 Src_IP: 9.1.1.1
Dest_IP: 225.0.0.1 Type: V2_Membership_Report Group: 225.0.0.1
```

The following parameters are displayed in the trace message:

Parameter	*Definition*
TX	A packet transmitted by the device.
Intf	The interface that the packet went out on. Format used is unit/slot/port (internal interface number). Unit is always shown as 1 for interfaces on a non-stacking device.
Src_Mac	Source MAC address of the packet.
Dest_Mac	Destination multicast MAC address of the packet.
Src_IP	The source IP address in the IP header in the packet.
Dest_IP	The destination multicast IP address in the packet.
Type	The type of IGMP packet. Type can be one of the following: • `Membership Query` – IGMP Membership Query • `V1_Membership_Report` – IGMP Version 1 Membership Report • `V2_Membership_Report` – IGMP Version 2 Membership Report • `V3_Membership_Report` – IGMP Version 3 Membership Report • `V2_Leave_Group` – IGMP Version 2 Leave Group
Group	Multicast group address in the IGMP header.

no debug igmpsnooping transmit

This command disables tracing of transmitted IGMP snooping packets.

Format `no debug igmpsnooping transmit`

Mode Privileged EXEC

debug igmpsnooping packet receive

This command enables tracing of IGMP Snooping packets received by the switch. Snooping should be enabled on the device and the interface in order to monitor packets for a particular interface.

Default disabled

Format `debug igmpsnooping packet receive`

Mode Privileged EXEC

A sample output of the trace message is shown below.

```
<15> JAN 01 02:45:06 192.168.17.29-1 IGMPSNOOP[185429992]: igmp_snooping_debug.c(116) 908 % Pkt RX
- Intf: 1/0/20(20), Vlan_Id:1 Src_Mac: 00:03:0e:00:00:10 Dest_Mac: 01:00:5e:00:00:05 Src_IP:
11.1.1.1 Dest_IP: 225.0.0.5 Type: Membership_Query Group: 225.0.0.5
```

The following parameters are displayed in the trace message:

Parameter	*Definition*
RX	A packet received by the device.
Intf	The interface that the packet went out on. Format used is unit/slot/port (internal interface number). Unit is always shown as 1 for interfaces on a non-stacking device.
Src_Mac	Source MAC address of the packet.
Dest_Mac	Destination multicast MAC address of the packet.
Src_IP	The source IP address in the ip header in the packet.
Dest_IP	The destination multicast ip address in the packet.
Type	The type of IGMP packet. Type can be one of the following: • `Membership_Query` – IGMP Membership Query • `V1_Membership_Report` – IGMP Version 1 Membership Report • `V2_Membership_Report` – IGMP Version 2 Membership Report • `V3_Membership_Report` – IGMP Version 3 Membership Report • `V2_Leave_Group` – IGMP Version 2 Leave Group
Group	Multicast group address in the IGMP header.

no debug igmpsnooping receive

This command disables tracing of received IGMP Snooping packets.

Format `no debug igmpsnooping receive`

Mode Privileged EXEC

debug ip acl

Use this command to enable debug of IP Protocol packets matching the ACL criteria.

Default disabled

Format `debug ip acl` *`acl Number`*

Mode Privileged EXEC

no debug ip acl

Use this command to disable debug of IP Protocol packets matching the ACL criteria.

Format `no debug ip acl acl Number`

Mode Privileged EXEC

debug ip dvmrp packet

Use this command to trace DVMRP packet reception and transmission. **receive** traces only received DVMRP packets and **transmit** traces only transmitted DVMRP packets. When neither keyword is used in the command, then all DVMRP packet traces are dumped. Vital information such as source address, destination address, control packet type, packet length, and the interface on which the packet is received or transmitted is displayed on the console

Default disabled

Format `debug ip dvmrp packet [receive | transmit]`

Mode Privileged EXEC

no debug ip dvmrp packet

Use this command to disable debug tracing of DVMRP packet reception and transmission.

Format `no debug ip dvmrp packet [receive | transmit]`

Mode Privileged EXEC

debug ip igmp packet

Use this command to trace IGMP packet reception and transmission. **receive** traces only received IGMP packets and **transmit** traces only transmitted IGMP packets. When neither keyword is used in the command, then all IGMP packet traces are dumped. Vital information such as source address, destination address, control packet type, packet length, and the interface on which the packet is received or transmitted is displayed on the console.

Default disabled

Format `debug ip igmp packet [receive | transmit]`

Mode Privileged EXEC

no debug ip igmp packet

Use this command to disable debug tracing of IGMP packet reception and transmission.

Format `no debug ip igmp packet [receive | transmit]`

Mode Privileged EXEC

debug ip mcache packet

Use this command for tracing MDATA packet reception and transmission. **receive** traces only received data packets and **transmit** traces only transmitted data packets. When neither keyword is used in the command, then all data packet traces are dumped. Vital information such as source address, destination address, packet length, and the interface on which the packet is received or transmitted is displayed on the console.

Default disabled

Format `debug ip mcache packet [receive | transmit]`

Mode Privileged EXEC

no debug ip mcache packet

Use this command to disable debug tracing of MDATA packet reception and transmission.

Format `no debug ip mcache packet [receive | transmit]`

Mode Privileged EXEC

debug ip pimdm packet

Use this command to trace PIMDM packet reception and transmission. **receive** traces only received PIMDM packets and **transmit** traces only transmitted PIMDM packets. When neither keyword is used in the command, then all PIMDM packet traces are dumped. Vital information such as source address, destination address, control packet type, packet length, and the interface on which the packet is received or transmitted is displayed on the console.

Default disabled

Format `debug ip pimdm packet [receive | transmit]`

Mode Privileged EXEC

no debug ip pimdm packet

Use this command to disable debug tracing of PIMDM packet reception and transmission.

Format `no debug ip pimdm packet [receive | transmit]`

Mode Privileged EXEC

debug ip pimsm packet

Use this command to trace PIMSM packet reception and transmission. **receive** traces only received PIMSM packets and **transmit** traces only transmitted PIMSM packets. When neither keyword is used in the command, then all PIMSM packet traces are dumped. Vital information such as source address, destination address, control packet type, packet length, and the interface on which the packet is received or transmitted is displayed on the console.

Default disabled

Format `debug ip pimsm packet [receive | transmit]`

Mode Privileged EXEC

no debug ip pimsm packet

Use this command to disable debug tracing of PIMSM packet reception and transmission.

Format `no debug ip pimsm packet [receive | transmit]`

Mode Privileged EXEC

debug ip vrrp

Use this command to enable VRRP debug protocol messages.

Default disabled

Format `debug ip vrrp`

Mode Privileged EXEC

no debug ip vrrp

Use this command to disable VRRP debug protocol messages.

Format `no debug ip vrrp`

Mode Privileged EXEC

debug ipv6 dhcp

This command displays debug information about DHCPv6 client activities and traces DHCPv6 packets to and from the local DHCPv6 client.

Default disabled

Format `debug ipv6 dhcp`

Mode Privileged EXEC

no ipv6 debug dhcp

This command disables the display of debug trace output for DHCPv6 client activity.

Format `no debug ipv6 dhcp`

Mode Privileged EXEC

debug ipv6 mcache packet

Use this command for tracing MDATAv6 packet reception and transmission. **receive** traces only received data packets and **transmit** traces only transmitted data packets. When neither keyword is used in the command, then all data packet traces are dumped. Vital information such as source address, destination address, packet length, and the interface on which the packet is received or transmitted is displayed on the console.

Default disabled

Format `debug ipv6 mcache packet [receive | transmit]`

Mode Privileged EXEC

no debug ipv6 mcache packet

Use this command to disable debug tracing of MDATAv6 packet reception and transmission.

Format `no debug ipv6 mcache packet [receive | transmit]`

Mode Privileged EXEC

debug ipv6 mld packet

Use this command to trace MLDv6 packet reception and transmission. **receive** traces only received MLDv6 packets and **transmit** traces only transmitted MLDv6 packets. When neither keyword is used in the command, then all MLDv6 packet traces are dumped. Vital information such as source address, destination address, control packet type, packet length, and the interface on which the packet is received or transmitted is displayed on the console.

Default disabled

Format `debug ipv6 mld packet [receive | transmit]`

Mode Privileged EXEC

no debug ipv6 mld packet

Use this command to disable debug tracing of MLDv6 packet reception and transmission.

Format `no debug ipv6 mld packet [receive | transmit]`

Mode Privileged EXEC

debug ipv6 pimdm packet

Use this command to trace PIMDMv6 packet reception and transmission. **receive** traces only received PIMDMv6 packets and **transmit** traces only transmitted PIMDMv6 packets. When neither keyword is used in the command, then all PIMDMv6 packet traces are dumped. Vital information such as source address, destination address, control packet type, packet length, and the interface on which the packet is received or transmitted is displayed on the console.

Default disabled

Format `debug ipv6 pimdm packet [receive | transmit]`

Mode Privileged EXEC

no debug ipv6 pimdm packet

Use this command to disable debug tracing of PIMDMv6 packet reception and transmission.

debug ipv6 pimsm packet

Use this command to trace PIMSMv6 packet reception and transmission. **receive** traces only received PIMSMv6 packets and **transmit** traces only transmitted PIMSMv6 packets. When neither keyword is used in the command, then all PIMSMv6 packet traces are dumped. Vital information such as source address, destination address, control packet type, packet length, and the interface on which the packet is received or transmitted is displayed on the console.

Default disabled

Format `debug ipv6 pimsm packet [receive | transmit]`

Mode Privileged EXEC

no debug ipv6 pimsm packet

Use this command to disable debug tracing of PIMSMv6 packet reception and transmission.

Format `no debug ipv6 pimsm packet [receive | transmit]`

Mode Privileged EXEC

debug lacp packet

This command enables tracing of LACP packets received and transmitted by the switch.

Default	disabled
Format	`debug lacp packet`
Mode	Privileged EXEC

A sample output of the trace message is shown below.

```
<15> JAN 01 14:04:51 10.254.24.31-1 DOT3AD[183697744]: dot3ad_debug.c(385) 58 %%
 Pkt TX - Intf: 1/0/1(1), Type: LACP, Sys: 00:11:88:14:62:e1, State: 0x47, Key:
0x36
```

no debug lacp packet

This command disables tracing of LACP packets.

Format	`no debug lacp packet`
Mode	Privileged EXEC

debug mldsnooping packet

Use this command to trace MLD snooping packet reception and transmission. **receive** traces only received MLD snooping packets and **transmit** traces only transmitted MLD snooping packets. When neither keyword is used in the command, then all MLD snooping packet traces are dumped. Vital information such as source address, destination address, control packet type, packet length, and the interface on which the packet is received or transmitted is displayed on the console.

Default	disabled
Format	`debug mldsnooping packet [receive | transmit]`
Mode	Privileged EXEC

no debug mldsnooping packet

Use this command to disable debug tracing of MLD snooping packet reception and transmission.

debug ospf packet

This command enables tracing of OSPF packets received and transmitted by the switch.

Default disabled

Format `debug ospf packet`

Mode Privileged EXEC

Sample outputs of the trace messages are shown below.

```
<15> JAN 02 11:03:31 10.50.50.1-2 OSPF[46300472]: ospf_debug.c(297) 25430 % Pkt RX - Intf:2/0/48 Src
Ip:192.168.50.2 DestIp:224.0.0.5 AreaId:0.0.0.0 Type:HELLO NetMask:255.255.255.0 D
esigRouter:0.0.0.0 Backup:0.0.0.0

<15> JAN 02 11:03:35 10.50.50.1-2 OSPF[46300472]: ospf_debug.c(293) 25431 % Pkt TX - Intf:2/0/48 Src
Ip:10.50.50.1 DestIp:192.168.50.2 AreaId:0.0.0.0 Type:DB_DSCR Mtu:1500 Options:E
Flags: I/M/MS Seq:126166

<15> JAN 02 11:03:36 10.50.50.1-2 OSPF[46300472]: ospf_debug.c(297) 25434 % Pkt RX - Intf:2/0/48 Src
Ip:192.168.50.2 DestIp:192.168.50.1 AreaId:0.0.0.0 Type:LS_REQ Length: 1500

<15> JAN 02 11:03:36 10.50.50.1-2 OSPF[46300472]: ospf_debug.c(293) 25435 % Pkt TX - Intf:2/0/48 Src
Ip:10.50.50.1 DestIp:192.168.50.2 AreaId:0.0.0.0 Type:LS_UPD Length: 1500

<15> JAN 02 11:03:37 10.50.50.1-2 OSPF[46300472]: ospf_debug.c(293) 25441 % Pkt TX - Intf:2/0/48 Src
Ip:10.50.50.1 DestIp:224.0.0.6 AreaId:0.0.0.0 Type:LS_ACK Length: 1500
```

The following parameters are displayed in the trace message:

Parameter	*Definition*
TX/RX	TX refers to a packet transmitted by the device. RX refers to packets received by the device.
Intf	The interface that the packet came in or went out on. Format used is unit/slot/port (internal interface number).
SrcIp	The source IP address in the IP header of the packet.
DestIp	The destination IP address in the IP header of the packet.
AreaId	The area ID in the OSPF header of the packet.
Type	Could be one of the following: `HELLO` – Hello packet `DB_DSCR` – Database descriptor `LS_REQ` – LS Request `LS_UPD` – LS Update `LS_ACK` – LS Acknowledge

The remaining fields in the trace are specific to the type of OSPF Packet.

HELLO packet field definitions:

Parameter	*Definition*
Netmask	The netmask in the hello packet.
DesignRouter	Designated Router IP address.
Backup	Backup router IP address.

DB_DSCR packet field definitions:

Field	*Definition*
MTU	MTU
Options	Options in the OSPF packet.
Flags	Could be one or more of the following: • I – Init • M – More • MS – Master/Slave
Seq	Sequence Number of the DD packet.

LS_REQ packet field definitions.

Field	*Definition*
Length	Length of packet

LS_UPD packet field definitions.

Field	*Definition*
Length	Length of packet

LS_ACK packet field definitions.

Field	*Definition*
Length	Length of packet

no debug ospf packet

This command disables tracing of OSPF packets.

Format `no debug ospf packet`

Mode Privileged EXEC

debug ospfv3 packet

Use this command to enable OSPFv3 packet debug trace.

Default disabled

Format `debug ospfv3 packet`

Mode Privileged EXEC

no debug ospfv3 packet

Use this command to disable tracing of OSPFv3 packets.

Format `no debug ospfv3 packet`

Mode Privileged EXEC

debug ping packet

This command enables tracing of ICMP echo requests and responses. The command traces pings on the network port/ serviceport for switching packages. For routing packages, pings are traced on the routing ports as well.

Default disabled

Format `debug ping packet`

Mode Privileged EXEC

A sample output of the trace message is shown below.

```
<15> JAN 01 00:21:22 192.168.17.29-1 SIM[181040176]: sim_debug.c(128) 20 % Pkt TX - Intf: 1/0/1(1), SRC_IP:10.50.50.2, DEST_IP:10.50.50.1, Type:ECHO_REQUEST


<15> JAN 01 00:21:22 192.168.17.29-1 SIM[182813968]: sim_debug.c(82) 21 % Pkt RX - Intf: 1/0/1(1), SRC_IP:10.50.50.1, DEST_IP:10.50.50.2, Type:ECHO_REPLY
```

The following parameters are displayed in the trace message:

Parameter	*Definition*
TX/RX	TX refers to a packet transmitted by the device. RX refers to packets received by the device.
Intf	The interface that the packet came in or went out on. Format used is unit/slot/port (internal interface number). Unit is always shown as 1 for interfaces on a non-stacking device.
SRC_IP	The source IP address in the IP header in the packet.
DEST_IP	The destination IP address in the IP header in the packet.
Type	Type determines whether or not the ICMP message is a REQUEST or a RESPONSE.

no debug ping packet

This command disables tracing of ICMP echo requests and responses.

Format `no debug ping packet`

Mode Privileged EXEC

debug rip packet

This command turns on tracing of RIP requests and responses. This command takes no options. The output is directed to the log file.

Default disabled

Format `debug rip packet`

Mode Privileged EXEC

A sample output of the trace message is shown below.

```
<15> JAN 01 00:35:15 192.168.17.29-1 RIP[181783160]: rip_map_debug.c(96) 775 %
Pkt RX on Intf: 1/0/1(1), Src_IP:43.1.1.1 Dest_IP:43.1.1.2
Rip_Version: RIPv2 Packet_Type:RIP_RESPONSE
ROUTE 1): Network: 10.1.1.0 Mask: 255.255.255.0 Metric: 1
ROUTE 2): Network: 40.1.0.0 Mask: 255.255.0.0 Metric: 1
ROUTE 3): Network: 10.50.50.0 Mask: 255.255.255.0 Metric: 1
ROUTE 4): Network: 41.1.0.0 Mask: 255.255.0.0 Metric: 1
ROUTE 5): Network:42.0.0.0 Mask:255.0.0.0 Metric:1
Another 6 routes present in packet not displayed.
```

The following parameters are displayed in the trace message:

Parameter	*Definition*
TX/RX	TX refers to a packet transmitted by the device. RX refers to packets received by the device.
Intf	The interface that the packet came in or went out on. Format used is unit/slot/port (internal interface number). Unit is always shown as 1 for interfaces on a non-stacking device.
Src_IP	The source IP address in the IP header of the packet.
Dest_IP	The destination IP address in the IP header of the packet.
Rip_Version	RIP version used: RIPv1 or RIPv2.
Packet_Type	Type of RIP packet: RIP_REQUEST or RIP_RESPONSE.
Routes	Up to 5 routes in the packet are displayed in the following format: `Network:` *a.b.c.d* `Mask` *a.b.c.d* `Next_Hop` *a.b.c.d* `Metric` *a* The next hop is only displayed if it is different from `0.0.0.0`. For RIPv1 packets, Mask is always `0.0.0.0`.
Number of routes not printed	Only the first five routes present in the packet are included in the trace. There is another notification of the number of additional routes present in the packet that were not included in the trace.

no debug rip packet

This command disables tracing of RIP requests and responses.

Format `no debug rip packet`

Mode Privileged EXEC

debug sflow packet

Use this command to enable sFlow debug packet trace.

Default disabled

Format `debug sflow packet`

Mode Privileged EXEC

no debug sflow packet

Use this command to disable sFlow debug packet trace.

Format `no debug sflow packet`

Mode Privileged EXEC

debug spanning-tree bpdu

This command enables tracing of spanning tree BPDUs received and transmitted by the switch.

Default disabled

Format `debug spanning-tree bpdu`

Mode Privileged EXEC

no debug spanning-tree bpdu

This command disables tracing of spanning tree BPDUs.

Format `no debug spanning-tree bpdu`

Mode Privileged EXEC

debug spanning-tree bpdu receive

This command enables tracing of spanning tree BPDUs received by the switch. Spanning tree should be enabled on the device and on the interface in order to monitor packets for a particular interface.

Default disabled

Format `debug spanning-tree bpdu receive`

Mode Privileged EXEC

A sample output of the trace message is shown below.

```
<15> JAN 01 01:02:04 192.168.17.29-1 DOT1S[191096896]: dot1s_debug.c(1249) 101 % Pkt RX - Intf: 1/
0/9(9), Source_Mac: 00:11:88:4e:c2:10 Version: 3, Root Mac: 00:11:88:4e:c2:00, Root Priority: 0x8000
Path Cost: 0
```

The following parameters are displayed in the trace message:

Parameter	*Definition*
RX	A packet received by the device.
Intf	The interface that the packet came in on. Format used is unit/port/slot (internal interface number). Unit is always shown as 1 for interfaces on a non-stacking device.
Source_Mac	Source MAC address of the packet.
Version	Spanning tree protocol version (0–3). 0 refers to STP, 2 RSTP and 3 MSTP.
Root_Mac	MAC address of the CIST root bridge.
Root_Priority	Priority of the CIST root bridge. The value is between 0 and 61440. It is displayed in hex in multiples of 4096.
Path_Cost	External root path cost component of the BPDU.

no debug spanning-tree bpdu receive

This command disables tracing of received spanning tree BPDUs.

Format `no debug spanning-tree bpdu receive`

Mode Privileged EXEC

debug spanning-tree bpdu transmit

This command enables tracing of spanning tree BPDUs transmitted by the switch. Spanning tree should be enabled on the device and on the interface in order to monitor packets on a particular interface.

Default disabled

Format `debug spanning-tree bpdu transmit`

Mode Privileged EXEC

A sample output of the trace message is shown below.

```
<15> JAN 01 01:02:04 192.168.17.29-1 DOT1S[191096896]: dot1s_debug.c(1249) 101 % Pkt TX - Intf: 1/
0/7(7), Source_Mac: 00:11:88:4e:c2:00 Version: 3, Root_Mac: 00:11:88:4e:c2:00, Root_Priority: 0x8000
Path_Cost: 0
```

The following parameters are displayed in the trace message:

Parameter	*Definition*
TX	A packet transmitted by the device.
Intf	The interface that the packet went out on. Format used is unit/port/slot (internal interface number). Unit is always shown as 1 for interfaces on a non-stacking device.
Source_Mac	Source MAC address of the packet.
Version	Spanning tree protocol version (0–3). 0 refers to STP, 2 RSTP and 3 MSTP.
Root_Mac	MAC address of the CIST root bridge.
Root_Priority	Priority of the CIST root bridge. The value is between 0 and 61440. It is displayed in hex in multiples of 4096.
Path_Cost	External root path cost component of the BPDU.

no debug spanning-tree bpdu transmit

This command disables tracing of transmitted spanning tree BPDUs.

Format `no debug spanning-tree bpdu transmit`

Mode Privileged EXEC

logging persistent

Use this command to configure the Persistent logging for the switch. The severity level of logging messages is specified at severity level. Possible values for severity level are (emergency|0, alert|1, critical|2, error|3, warning|4, notice|5, info|6, debug|7).

Default Disable

Format `logging persistent` *`severity level`*

Mode Global Config

no logging persistent

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

Format `no logging persistent`

Mode Global Config

Cable Test Command

The cable test feature enables you to determine the cable connection status on a selected port.

Note: The cable test feature is supported only for copper cable. It is not supported for optical fiber cable.

If the port has an active link while the cable test is run, the link can go down for the duration of the test.

cablestatus

This command returns the status of the specified port.

Format `cablestatus` *`unit/slot/port`*

Mode Privileged EXEC

Field	*Description*
Cable Status	One of the following statuses is returned: • **Normal**: The cable is working correctly. • **Open**: The cable is disconnected or there is a faulty connector. • **Short**: There is an electrical short in the cable. • **Cable Test Failed**: The cable status could not be determined. The cable may in fact be working.
Cable Length	If this feature is supported by the PHY for the current link speed, the cable length is displayed as a range between the shortest estimated length and the longest estimated length. Note that if the link is down and a cable is attached to a 10/100 Ethernet adapter, then the cable status may display as Open or Short because some Ethernet adapters leave unused wire pairs unterminated or grounded. Unknown is displayed if the cable length could not be determined.

sFlow Commands

sFlow® is the standard for monitoring high-speed switched and routed networks. sFlow technology is built into network equipment and gives complete visibility into network activity, enabling effective management and control of network resources.

sflow receiver

Use this command to configure the sFlow collector parameters (owner string, receiver timeout, max datagram size, IP address, and port).

Format `sflow receiver rcvr_idx owner owner-string timeout rcvr_timeout max datagram size ip/ipv6 ip port port`

Mode Global Config

Field	*Description*
Receiver Owner	The identity string for the receiver, the entity making use of this sFlowRcvrTable entry. The range is 127 characters. The default is a null string. The empty string indicates that the entry is currently unclaimed and the receiver configuration is reset to the default values. An entity wishing to claim an sFlowRcvrTable entry must ensure that the entry is unclaimed before trying to claim it. The entry is claimed by setting the owner string to a non-null value. The entry must be claimed before assigning a receiver to a sampler or poller.
Receiver Timeout	The time, in seconds, remaining before the sampler or poller is released and stops sending samples to receiver. A management entity wanting to maintain control of the sampler is responsible for setting a new value before the old one expires. The allowed range is 0–4294967295 seconds. The default is zero (0).
Receiver Max Datagram Size	The maximum number of data bytes that can be sent in a single sample datagram. The management entity should set this value to avoid fragmentation of the sFlow datagrams. The allowed range is 200 to 9116). The default is 1400.
Receiver IP	The sFlow receiver IP address. If set to 0.0.0.0, no sFlow datagrams will be sent. The default is 0.0.0.0.
Receiver Port	The destination Layer4 UDP port for sFlow datagrams. The range is 1–65535. The default is 6343.

no sflow receiver

Use this command to set the sFlow collector parameters back to the defaults.

Format `no sflow receiver indx {ip ip-address | maxdatagram size | owner string timeout interval | port 14-port}`

Mode Global Config

sflow sampler

A data source configured to collect flow samples is called a poller. Use this command to configure a new sFlow sampler instance on an interface or range of interfaces for this data source if *rcvr_idx* is valid.

Format `sflow sampler {rcvr-indx | rate sampling-rate | maxheadersize size}`

Mode Interface Config

Field	*Description*
Receiver Index	The sFlow Receiver for this sFlow sampler to which flow samples are to be sent. A value of zero (0) means that no receiver is configured, no packets will be sampled. Only active receivers can be set. If a receiver expires, then all samplers associated with the receiver will also expire. Possible values are 1–8. The default is 0.
Maxheadersize	The maximum number of bytes that should be copied from the sampler packet. The range is 20–256. The default is 128. When set to zero (0), all the sampler parameters are set to their corresponding default value.
Sampling Rate	The statistical sampling rate for packet sampling from this source. A sampling rate of 1 counts all packets. A value of zero (0) disables sampling. A value of N means that out of N incoming packets, 1 packet will be sampled. The range is 1024–65536 and 0. The default is 0.

no sflow sampler

Use this command to reset the sFlow sampler instance to the default settings.

Format `no sflow sampler {rcvr-indx | rate sampling-rate | maxheadersize size}`

Mode Interface Config

sflow poller

A data source configured to collect counter samples is called a poller. Use this command to enable a new sFlow poller instance on an interface or range of interfaces for this data source if *rcvr_idx* is valid.

Format `sflow poller {rcvr-indx | interval poll-interval}`

Mode Interface Config

Field	*Description*
Receiver Index	Enter the sFlow Receiver associated with the sampler/poller. A value of zero (0) means that no receiver is configured. The range is 1–8. The default is 0.
Poll Interval	Enter the sFlow instance polling interval. A poll interval of zero (0) disables counter sampling. When set to zero (0), all the poller parameters are set to their corresponding default value. The range is 0–86400. The default is 0. A value of N means once in N seconds a counter sample is generated.

no sflow poller

Use this command to reset the sFlow poller instance to the default settings.

Format `no sflow poller {rcvr-indx | interval poll-interval}`

Mode Interface Config

show sflow agent

The sFlow agent collects time-based sampling of network interface statistics and flow-based samples. These are sent to the configured sFlow receivers. Use this command to display the sFlow agent information.

Format `show sflow agent`

Mode Privileged EXEC

Field	*Description*
sFlow Version	Uniquely identifies the version and implementation of this MIB. The version string must have the following structure: MIB Version; Organization; Software Revision where: • MIB Version: 1.3, the version of this MIB. • Organization: Broadcom Corp. • Revision: 1.0
IP Address	The IP address associated with this agent.

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

```
(switch) #show sflow agent

sFlow Version..................................... 1.3;Broadcom Corp;1.0
IP Address........................................ 10.131.12.66
```

show sflow pollers

Use this command to display the sFlow polling instances created on the switch. Use "-" for range.

Format `show sflow pollers`

Mode Privileged EXEC

Field	*Description*
Poller Data Source	The sFlowDataSource (slot/port) for this sFlow sampler. This agent will support Physical ports only.
Receiver Index	The sFlowReceiver associated with this sFlow counter poller.
Poller Interval	The number of seconds between successive samples of the counters associated with this data source.

show sflow receivers

Use this command to display configuration information related to the sFlow receivers.

Format `show sflow receivers [index]`

Mode Privileged EXEC

Field	*Description*
Receiver Index	The sFlow Receiver associated with the sampler/poller.
Owner String	The identity string for receiver, the entity making use of this sFlowRcvrTable entry.
Time Out	The time (in seconds) remaining before the receiver is released and stops sending samples to sFlow receiver.
Max Datagram Size	The maximum number of bytes that can be sent in a single sFlow datagram.
Port	The destination Layer4 UDP port for sFlow datagrams.
IP Address	The sFlow receiver IP address.
Address Type	The sFlow receiver IP address type. For an IPv4 address, the value is 1 and for an IPv6 address, the value is 2.
Datagram Version	The sFlow protocol version to be used while sending samples to sFlow receiver.

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

```
(switch) #show sflow receivers 1
Receiver Index.............................. 1
Owner String................................
Time out.................................... 0
IP Address:................................. 0.0.0.0
Address Type................................ 1
Port........................................ 6343
Datagram Version............................ 5
Maximum Datagram Size....................... 1400
```

show sflow samplers

Use this command to display the sFlow sampling instances created on the switch.

Format `show sflow samplers`

Mode Privileged EXEC

Field	*Description*
Sampler Data Source	The sFlowDataSource (slot/port) for this sFlow sampler. This agent will support Physical ports only.
Receiver Index	The sFlowReceiver configured for this sFlow sampler.
Packet Sampling Rate	The statistical sampling rate for packet sampling from this source.
Max Header Size	The maximum number of bytes that should be copied from a sampled packet to form a flow sample.

Switch Database Management Template Commands

A Switch Database Management (SDM) template is a description of the maximum resources a switch or router can use for various features. Different SDM templates allow different combinations of scaling factors, enabling different allocations of resources depending on how the device is used. In other words, SDM templates enable you to reallocate system resources to support a different mix of features based on your network requirements.

Note: If you attach a unit to a stack and its template does not match the stack's template, then the new unit will automatically reboot using the template used by other stack members. To avoid the automatic reboot, you may first set the template to the template used by existing members of the stack. Then power off the new unit, attach it to the stack, and power it on.

sdm prefer

Use this command to change the template that will be active after the next reboot. The keywords are as follows:

- **dual-ipv4-and-ipv6** — filters subsequent template choices to those that support both IPv4 and IPv6. There is only one such template, and it is selected using the keyword default.
- **ipv4-routing** — filters subsequent template choices to those that support IPv4, and not IPv6. The default IPv4-only template maximizes the number of IPv4 unicast routes, while limiting the number of ECMP next hops in each route to 4. The data-center template supports increases the number of ECMP next hops to 16 and reduces the number of routes.

Note: After setting the template, you must reboot in order for the configuration change to take effect.

Default	dual IPv4 and IPv6 template
Format	*sdm prefer {dual-ipv4-and-ipv6 default | ipv4-routing {default | data-center}}*
Mode	Global Config

no sdm prefer

Use this command to revert to the default template after the next reboot.

Format	`no sdm prefer`
Mode	Global Config

show sdm prefer

Use this command to view the currently active SDM template and its scaling parameters, or to view the scaling parameters for an inactive template. When invoked with no optional keywords, this command lists the currently active template and the template that will become active on the next reboot, if it is different from the currently active template. If the system boots with a non-default template, and you clear the template configuration, either using `no sdm prefer` or by deleting the startup configuration, `show sdm prefer` lists the default template as the next active template.

Use the optional keywords to list the scaling parameters of a specific template.

Format `show sdm prefer [dual-ipv4-and-ipv6 default | ipv4-routing {default | data-center}]`

Mode Privileged EXEC

Field	*Description*
ARP Entries	The maximum number of entries in the IPv4 Address Resolution Protocol (ARP) cache for routing interfaces.
IPv4 Unicast Routes	The maximum number of IPv4 unicast forwarding table entries.
IPv6 NDP Entries	The maximum number of IPv6 Neighbor Discovery Protocol (NDP) cache entries.
IPv6 Unicast Routes	The maximum number of IPv6 unicast forwarding table entries.
ECMP Next Hops	The maximum number of next hops that can be installed in the IPv4 and IPv6 unicast forwarding tables.
IPv4 Multicast Routes	The maximum number of IPv4 multicast forwarding table entries.
IPv6 Multicast Routes	The maximum number of IPv6 multicast forwarding table entries.

Example:

```
#show sdm prefer

The current template is the Dual IPv4 and IPv6 template.

ARP Entries..................................... 4096
IPv4 Unicast Routes............................. 6112
IPv6 NDP Entries................................ 2048
IPv6 Unicast Routes............................. 3072
ECMP Next Hops.................................. 4
IPv4 Multicast Routes........................... 256
IPv6 Multicast Routes........................... 256
```

Green Ethernet Commands

This section describes the commands you use to configure Green Ethernet modes on the system. The purpose of the Green Ethernet features is to save power. DWS-4000 software supports the following three Green Ethernet modes:

- Energy-detect mode
- Short-reach mode
- Energy-efficient Ethernet (EEE) mode

Note: Support for each Green Ethernet mode is platform dependent. The features and commands described in this section might not be available on your switch.

green-mode energy-detect

Use this command to enable energy-detect mode on an interface or on a range of interfaces. With this mode enabled, when the port link is down, the port automatically powers down for short period of time and then wakes up to check link pulses. In energy-detect mode, the port can perform auto-negotiation and consume less power when no link partner is present.

Default	disabled
Format	`green-mode energy-detect`
Mode	Interface Config

no green-mode energy-detect

Use this command to disable energy-detect mode on the interface(s).

Format	`no green-mode energy-detect`
Mode	Interface Config

green-mode short-reach

Use this command to enable short reach mode on an interface or on a range of interfaces. Short-reach mode enables the port to enter low-power mode if the length of the cable is less than 10m. Use the `auto` keyword to enable short-reach mode automatically on detection of cable length less than 10m, and/or use the `force` keyword to force the port into short-reach mode.

Note: The `green-mode short-reach` command allows you to enable both forced and auto short-reach modes simultaneously, but auto mode is practically ineffective when force mode is also enabled on the interface.

Default disabled

Format `green-mode short-reach {[auto] [force]}`

Mode Interface Config

no green-mode short-reach

Use this command to disable short-reach mode on the interface(s).

Format `no green-mode short-reach {[auto] [force]}`

Mode Interface Config

green-mode eee

Use this command to enable EEE low-power idle mode on an interface or on a range of interfaces. The EEE mode enables both send and receive sides of the link to disable some functionality for power saving when lightly loaded. The transition to EEE low-power mode does not change the port link status. Frames in transit are not dropped or corrupted in transition to and from this mode.

Default disabled

Format `green-mode eee`

Mode Interface Config

no green-mode eee

Use this command to disable EEE mode on the interface(s).

Format `no green-mode eee`

Mode Interface Config

green-mode eee tx-idle-time

Use this command to configure the EEE mode transmit idle time for an interface or range of interfaces. The idle time is in microseconds. The transmit idle time is the amount of time the port waits before moving to the MAC TX transitions to the LPI state.

Note: This command is not available on all systems, even if EEE mode is supported.

Default 0

Format `green-mode eee tx-idle-time` *`0–4294977295`*

Mode Interface Config

no green-mode eee tx-idle-time

Use this command to return the EEE idle time to the default value.

Format `no green-mode eee tx-idle-time`

Mode Interface Config

green-mode eee tx-wake-time

Use this command to configure the EEE mode transmit wake time for an interface or range of interfaces. The wake time is in microseconds. The transmit wake time is the amount of time the switch must wait to go back to the ACTIVE state from the LPI state when it receives a packet for transmission.

Note: This command is not available on all systems, even if EEE mode is supported.

Default 0

Format `green-mode eee tx-wake-time` *`0–65535`*

Mode Interface Config

no green-mode eee tx-wake-time

Use this command to return the EEE wake time to the default value.

Format `no green-mode eee tx-wake-time`

Mode Interface Config

green-mode eee-lpi-history sampling-interval

Use this command to configure global EEE LPI history collection interval for the system. The value specified in this command is applied globally on all interfaces in the switch or stack of switches. The sampling interval unit is seconds.

Note: The sampling interval takes effect immediately; the current and future samples are collected at this new sampling interval.

Default 3600 seconds

Format `green-mode eee-lpi-history sampling-interval` *`30–36000`*

Mode Global Config

no green-mode eee-lpi-history sampling-interval

Use this command to return the global EEE LPI history collection interval to the default value.

Format `no green-mode eee-lpi-history sampling-interval`

Mode Global Config

green-mode eee-lpi-history max-samples

Use this command to configure global EEE LPI history collection buffer size for the system. The value specified in this command is applied globally on all interfaces in the switch or stack of switches.

Default 168

Format `green-mode eee-lpi-history max-samples` *`1–168`*`}`

Mode Global Config

no green-mode eee-lpi-history max samples

Use this command to return the global EEE LPI history collection buffer size to the default value.

Format `no green-mode eee-lpi-history max-samples`

Mode Global Config

show green-mode

Use this command to display the green-mode configuration and operational status on all ports or on the specified port.

Note: The fields that display in the `show green-mode` command output depend on the Green Ethernet modes available on the hardware platform.

Format `show green-mode [slot/port]`

Mode Privileged EXEC

If you do **not** specify a port, the command displays the information in the following table.

Term	*Definition*
Global	
Cumulative Energy Saving per Stack	Estimated Cumulative energy saved per stack in (Watts * hours) due to all green modes enabled
Current Power Consumption per Stack	Power Consumption by all ports in stack in mWatts.
Power Saving	Estimated Percentage Power saved on all ports in stack due to Green mode(s) enabled.
Unit	Unit Index of the stack member
Green Ethernet Features supported	List of Green Features supported on the given unit which could be one or more of the following: Energy-Detect (Energy Detect), Short-Reach (Short Reach), EEE (Energy Efficient Ethernet), LPI-History (EEE Low Power Idle History), LLDP-Cap-Exchg (EEE LLDP Capability Exchange), Pwr-Usg-Est (Power Usage Estimates).
Energy Detect	
Energy-detect Config	Energy-detect Admin mode is enabled or disabled
Energy-detect Opr	Energy detect mode is currently active or inactive. The energy detect mode may be administratively enabled, but the operational status may be inactive.
Short Reach	
Short-Reach- Config auto	Short reach auto Admin mode is enabled or disabled
Short-Reach- Config forced	Short reach forced Admin mode is enabled or disabled
Short-Reach Opr	Short reach mode is currently active or inactive. The short-reach mode may be administratively enabled, but the operational status may be inactive.
EEE	
EEE Config	EEE Admin Mode is enabled or disabled.

Example: The following shows example CLI display output for on a system that supports all Green Ethernet features.

```
(Routing) #show green-mode
```

```
Current Power Consumption (mW)..............  11172
Power Saving (%)............................  10
Cumulative Energy Saving /Stack (W * H)...  10

Unit  Green Ethernet Features Supported
----  -------------------------------
1     Energy-Detect Short-Reach EEE LPI-History LLDP-Cap-Exchg Pwr-Usg-Est

Interface     Energy-Detect      Short-Reach-Config    Short-Reach    EEE
             Config       Opr     Auto        Forced       Opr        Config
---------  ---------  ---------  ---------  ---------  -----------   --------
1/0/1      Enabled    Active     Enabled    Disabled   Inactive      Enabled
1/0/2      Enabled    Active     Enabled    Disabled   Inactive      Enabled
1/0/3      Enabled    Active     Enabled    Disabled   Inactive      Enabled
1/0/4      Enabled    Active     Enabled    Disabled   Inactive      Enabled
1/0/5      Enabled    Active     Enabled    Disabled   Inactive      Enabled
1/0/6      Enabled    Active     Enabled    Disabled   Inactive      Enabled
1/0/7      Enabled    Active     Enabled    Disabled   Inactive      Enabled
--More-- or (q)uit
```

If you specify the port, the command displays the information in the following table.

Term	*Definition*
Energy Detect	
Energy-detect admin mode	Energy-detect mode is enabled or disabled
Energy-detect operational status	Energy detect mode is currently active or inactive. The energy-detect mode may be administratively enabled, but the operational status may be inactive. The possible reasons for the status are described below.
Reason for Energy-detect current operational status	The energy detect mode may be administratively enabled, but the operational status may be inactive for one of the following reasons: • Port is currently operating in the fiber mode • Link is up. • Admin Mode Disabled If the energy-detect operational status is active, this field displays *No energy detected.*
Short Reach	
Short-reach auto Admin mode	Short reach auto mode is enabled or disabled
Short-reach force Admin mode	Short reach force mode is enabled or disabled
Short reach operational status	short reach mode is currently active or inactive. The short-reach mode may be administratively enabled, but the operational status may be inactive.

Term	*Definition*
Reason for Short Reach current operational status	The short-reach mode may be administratively enabled, but the operational status may be inactive for one of the following reasons: • Long cable >10m • Link Down • Fiber • Admin Mode Disabled • Not At GIG speed • Cable length Unknown If the short reach operational status is active, this field displays one of the following reasons: • Short cable < 10m • Forced
EEE	
EEE Admin Mode	EEE Admin Mode is enabled or disabled.
Transmit Idle Time	It is the time for which condition to move to LPI state is satisfied, at the end of which MAC TX transitions to LPI state. The Range is (0 to 429496729). The Default value is 0
Transmit Wake Time	It is the time for which MAC / switch has to wait to go back to ACTIVE state from LPI state when it receives packet for transmission. The Range is (0 to 65535).The Default value is 0.
Rx Low Power Idle Event Count	This field is incremented each time MAC RX enters LP IDLE state. Shows the total number of Rx LPI Events since EEE counters are last cleared.
Rx Low Power Idle Duration (μSec)	This field indicates duration of Rx LPI state in 10 μs increments. Shows the total duration of Rx LPI since the EEE counters are last cleared.
Tx Low Power Idle Event Count	This field is incremented each time MAC TX enters LP IDLE state. Shows the total number of Tx LPI Events since EEE counters are last cleared.
Rx Low Power Idle Duration (μSec)	This field indicates duration of Tx LPI state in 10 μs increments. Shows the total duration of Tx LPI since the EEE counters are last cleared.
Tw_sys_tx (μSec)	Integer that indicates the value of Tw_sys that the local system can support. This value is updated by the EEE DLL Transmitter state diagram.
Tw_sys Echo (μSec)	Integer that indicates the remote system's Transmit Tw_sys that was used by the local system to compute the Tw_sys that it wants to request from the remote system.
Tw_sys_rx (μSec)	Integer that indicates the value of Tw_sys that the local system requests from the remote system. This value is updated by the EEE Receiver L2 state diagram.
Tw_sys_rx Echo (μSec)	Integer that indicates the remote systems Receive Tw_sys that was used by the local system to compute the Tw_sys that it can support.
Fallback Tw_sys (μSec)	Integer that indicates the value of fallback Tw_sys that the local system requests from the remote system.
Remote Tw_sys_tx (μSec)	Integer that indicates the value of Tw_sys that the remote system can support.
Remote Tw_sys Echo (μSec)	Integer that indicates the value Transmit Tw_sys echoed back by the remote system.

Term	*Definition*
Remote Tw_sys_rx (μSec)	Integer that indicates the value of Tw_sys that the remote system requests from the local system.
Remote Tw_sys_rx Echo (μSec)	Integer that indicates the value of Receive Tw_sys echoed back by the remote system.
Remote Fallback Tw_sys (μSec)	Integer that indicates the value of fallback Tw_sys that the remote system is advertising.
Tx_dll_enabled	Initialization status of the EEE transmit Data Link Layer management function on the local system.
Tx_dll_ready	Data Link Layer ready: This variable indicates that the TX system initialization is complete and is ready to update/receive LLDPDU containing EEE TLV. This variable is updated by the local system software.
Rx_dll_enabled	Status of the EEE capability negotiation on the local system.
Rx_dll_ready	Data Link Layer ready: This variable indicates that the RX system initialization is complete and is ready to update/receive LLDPDU containing EEE TLV. This variable is updated by the local system software.
Cumulative Energy Saving	Estimated Cumulative energy saved on this port in (Watts × hours) due to all green modes enabled
Time Since Counters Last Cleared	Time Since Counters Last Cleared (since the time of power up, or after the `clear eee statistics` command is executed)

Example: The following shows example CLI display output for on a system that supports all Green Ethernet features.

```
(Routing) #show green-mode 1/0/1
Energy Detect Admin Mode..................... Enabled
    Operational Status....................... Active
    Reason................................... No Energy Detected

Auto Short Reach Admin Mode.................. Enabled
    Forced Short Reach Admin Mode............... Enabled
    Operational Status....................... Active
    Reason................................... Forced

EEE Admin Mode............................... Enabled
    Transmit Idle Time....................... 0
    Transmit Wake Time....................... 0
    Rx Low Power Idle Event Count............ 0
    Rx Low Power Idle Duration (uSec)........ 0
    Tx Low Power Idle Event Count............ 0
    Tx Low Power Idle Duration (uSec)........ 0
    Tw_sys_tx (usec)......................... XX
    Tw_sys_tx Echo(usec)..................... XX
    Tw_sys_rx (usec)......................... XX
    Tw_sys_tx Echo(usec)..................... XX
    Fallback Tw_sys (usec)................... XX
    Remote Tw_sys_tx (usec).................. XX
    Remote Tw_sys_tx Echo(usec).............. XX
    Remote Tw_sys_rx (usec).................. XX
    Remote Tw_sys_tx Echo(usec).............. XX
    Remote fallback Tw_sys (usec)............ XX
    Tx DLL enabled........................... Yes
```

```
Tx DLL ready.............................. Yes
Rx DLL enabled............................ Yes
Rx DLL ready.............................. Yes
Cumulative Energy Saving (W * H).......... XX
Time Since Counters Last Cleared......... 1 day 20 hr 47 min 34 sec
```

clear green-mode statistics

Use this command to clear the following Green Ethernet mode statistics:

- EEE LPI event count and LPI duration
- EEE LPI history table entries
- Cumulative power-savings estimates

You can clear the statistics for a specified port or for all ports.

Note: Executing `clear eee statistics` clears only the EEE Transmit, Receive LPI event count, LPI duration, and Cumulative Energy Savings Estimates of the port. Other status parameters that display after executing `show green-mode` (see "show green-mode" on page 206) retain their data.

Format `clear green-mode statistics {slot/port | all}`

Mode Privileged EXEC

show green-mode eee-lpi-history

Use this command to display interface green-mode EEE LPI history.

Format `green-mode eee-lpi-history interface slot/port`

Mode Privileged EXEC

Term	*Definition*
Sampling Interval	Interval at which EEE LPI statistics is collected.
Total No. of Samples to Keep	Maximum number of samples to keep
Percentage LPI time per stack	Percentage of Total time spent in LPI mode by all port in stack when compared to total time since reset.
Sample No.	Sample Index
Sample Time	Time since last reset
%time spent in LPI mode since last sample	Percentage of time spent in LPI mode on this port when compared to sampling interval
%time spent in LPI mode since last reset	Percentage of total time spent in LPI mode on this port when compared to time since reset.

Example: The following shows example CLI display output for the command on a system with the EEE

feature enabled.

```
(Routing) #show green-mode eee-lpi-history interface 1/0/1

Sampling Interval (sec)..................... 30
Total No. of Samples to Keep................. 168
Percentage LPI time per stack................ 29

                            Percentage of    Percentage of
Sample     Time Since       Time spent in   Time spent in
 No.       The Sample       LPI mode since   LPI mode since
          Was Recorded      last sample      last reset
------ -------------------  --------------   --------------
10      0d:00:00:13           3                2
9       0d:00:00:44           3                2
8       0d:00:01:15           3                2
7       0d:00:01:46           3                2
6       0d:00:02:18           3                2
5       0d:00:02:49           3                2
4       0d:00:03:20           3                2
3       0d:00:03:51           3                1
2       0d:00:04:22           3                1
1       0d:00:04:53           3                1
```

Section 5: Switching Commands

This chapter describes the switching commands available in the DWS-4000 CLI.

The Switching Commands chapter includes the following sections:

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

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

Port Configuration Commands

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

interface

This command gives you access to the Interface Config mode, which allows you to enable or modify the operation of an interface (port). You can also specify a range of ports to configure at the same time by specifying the starting slot/port and ending slot/port, separated by a hyphen.

Format `interface {slot/port | slot/port(startrange)-slot/port(endrange)}`

Mode Global Config

Example: The following example enters Interface Config mode for port 1/0/1:

```
(switch) #configure
(switch) (config)#interface 1/0/1
(switch) (interface 1/0/1)#
```

Example: The following example enters Interface Config mode for ports 1/0/1 through 1/0/4:

```
(switch) #configure
(switch) (config)#interface 1/0/1-1/0/4
(switch) (interface 1/0/1-1/0/4)#
```

auto-negotiate

This command enables automatic negotiation on a port or range of ports.

Default enabled

Format `auto-negotiate`

Mode Interface Config

no auto-negotiate

This command disables automatic negotiation on a port.

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

Format `no auto-negotiate`

Mode Interface Config

auto-negotiate all

This command enables automatic negotiation on all ports.

Default enabled

Format `auto-negotiate all`

Mode Global Config

no auto-negotiate all

This command disables automatic negotiation on all ports.

Format `no auto-negotiate all`

Mode Global Config

description

Use this command to create an alpha-numeric description of an interface or range of interfaces.

Format `description` *`description`*

Mode Interface Config

mtu

Use the `mtu` command to set the maximum transmission unit (MTU) size, in bytes, for frames that ingress or egress the interface. You can use the `mtu` command to configure jumbo frame support for physical and port-channel (LAG) interfaces. For the standard DWS-4000 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 410.

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

shutdown

This command disables a port or range of ports.

Note: You can use the `shutdown` command on physical and port-channel (LAG) interfaces, but not on VLAN routing interfaces.

Default	enabled
Format	`shutdown`
Mode	Interface Config

no shutdown

This command enables a port.

Format	`no shutdown`
Mode	Interface Config

shutdown all

This command disables all ports.

Note: You can use the `shutdown all` command on physical and port-channel (LAG) interfaces, but not on VLAN routing interfaces.

Default	enabled
Format	`shutdown all`
Mode	Global Config

no shutdown all

This command enables all ports.

Format	`no shutdown all`
Mode	Global Config

speed

This command sets the speed and duplex setting for an interface or range of interfaces.

Format `speed {100 | 10} {half-duplex | full-duplex}`

Mode Interface Config

Acceptable Values	*Definition*
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	*Definition*
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

Term	*Definition*
Interface	slot/port
Type	If not blank, this field indicates that this port is a special type of port. The possible values are: • **Mirror** — this port is a monitoring port. For more information, see "Port Mirroring" on page 312. • **PC Mbr**— this port is a member of a port-channel (LAG). • **Probe** — this port is a probe port.
Admin Mode	The Port control administration state. The port must be enabled in order for it to be allowed into the network. May be enabled or disabled. The factory default is enabled.
Physical Mode	The desired port speed and duplex mode. If auto-negotiation support is selected, then the duplex mode and speed is set from the auto-negotiation process. Note that the maximum capability of the port (full duplex -100M) is advertised. Otherwise, this object determines the port's duplex mode and transmission rate. The factory default is Auto.
Physical Status	The port speed and duplex mode.
Link Status	The Link is up or down.
Link Trap	This object determines whether or not to send a trap when link status changes. The factory default is enabled.
LACP Mode	LACP is enabled or disabled on this port.

Spanning Tree Protocol Commands

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

Note: STP is enabled on the switch and on all ports and LAGs by default.

Note: If STP is disabled, the system does not forward BPDU messages.

spanning-tree

This command sets the spanning-tree operational mode to enabled.

Default	enabled
Format	`spanning-tree`
Mode	Global Config

no spanning-tree

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

Format	`no spanning-tree`
Mode	Global Config

spanning-tree bpdufilter

Use this command to enable BPDU Filter on an interface or range of interfaces.

Default	disabled
Format	`spanning-tree bpdufilter`
Mode	Interface Config

no spanning-tree bpdufilter

Use this command to disable BPDU Filter on the interface or range of interfaces.

Default	disabled
Format	`no spanning-tree bpdufilter`
Mode	Interface Config

spanning-tree bpdufilter default

Use this command to enable BPDU Filter on all the edge port interfaces.

Default disabled
Format `spanning-tree bpdufilter`
Mode Global Config

no spanning-tree bpdufilter default

Use this command to disable BPDU Filter on all the edge port interfaces.

Default disabled
Format `no spanning-tree bpdufilter default`
Mode Global Config

spanning-tree bpduflood

Use this command to enable BPDU Flood on an interface or range of interfaces.

Default disabled
Format `spanning-tree bpduflood`
Mode Interface Config

no spanning-tree bpduflood

Use this command to disable BPDU Flood on the interface or range of interfaces.

Default disabled
Format `no spanning-tree bpduflood`
Mode Interface Config

spanning-tree bpduguard

Use this command to enable BPDU Guard on the switch.

Default disabled
Format `spanning-tree bpduguard`
Mode Global Config

no spanning-tree bpduguard

Use this command to disable BPDU Guard on the switch.

Default disabled

Format `no spanning-tree bpduguard`

Mode Global Config

spanning-tree bpdumigrationcheck

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

Format `spanning-tree bpdumigrationcheck {slot/port | all}`

Mode Global Config

spanning-tree configuration name

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

Default base MAC address in hexadecimal notation

Format `spanning-tree configuration name` *name*

Mode Global Config

no spanning-tree configuration name

This command resets the Configuration Identifier Name to its default.

Format `no spanning-tree configuration name`

Mode Global Config

spanning-tree configuration revision

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

Default 0

Format `spanning-tree configuration revision` *0—65535*

Mode Global Config

no spanning-tree configuration revision

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

Format `no spanning-tree configuration revision`

Mode Global Config

spanning-tree edgeport

This command specifies that an interface (or range of interfaces) is an Edge Port within the common and internal spanning tree. This allows this port to transition to Forwarding State without delay.

Format `spanning-tree edgeport`

Mode Interface Config

no spanning-tree edgeport

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

Format `no spanning-tree edgeport`

Mode Interface Config

spanning-tree forceversion

This command sets the Force Protocol Version parameter to a new value.

Default 802.1s

Format `spanning-tree forceversion {802.1d | 802.1s | 802.1w}`

Mode Global Config

- Use 802.1d to specify that the switch transmits ST BPDUs rather than MST BPDUs (IEEE 802.1d functionality supported).
- Use 802.1s to specify that the switch transmits MST BPDUs (IEEE 802.1s functionality supported).
- Use 802.1w to specify that the switch transmits RST BPDUs rather than MST BPDUs (IEEE 802.1w functionality supported).

no spanning-tree forceversion

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

Format `no spanning-tree forceversion`

Mode Global Config

spanning-tree forward-time

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

Default 15

Format `spanning-tree forward-time {4—30}`

Mode Global Config

no spanning-tree forward-time

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

Format `no spanning-tree forward-time`

Mode Global Config

spanning-tree guard

This command selects whether loop guard or root guard is enabled on an interface or range of interfaces. If neither is enabled, then the port operates in accordance with the multiple spanning tree protocol.

Default none

Format `spanning-tree guard {none | root | loop}`

Mode Interface Config

no spanning-tree guard

This command disables loop guard or root guard on the interface.

Format `no spanning-tree guard`

Mode Interface Config

spanning-tree hello-time

This command sets the Admin Hello Time parameter to a new value for the common and internal spanning tree. The hello time *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 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 x (Bridge Forward Delay - 1)*.

Default	20
Format	`spanning-tree max-age {6—40}`
Mode	Global Config

no spanning-tree max-age

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

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

spanning-tree max-hops

This command sets the 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 parameter *mstid* is a number within a range of 1 to 4094, that corresponds to the new instance ID to be added. The maximum number of multiple instances supported by the switch is 4.

Default none

Format `spanning-tree mst instance mstid`

Mode Global Config

no spanning-tree mst instance

This command removes a multiple spanning tree instance from the switch and reallocates all VLANs allocated to the deleted instance to the common and internal spanning tree. The parameter *mstid* is a number that corresponds to the desired existing multiple spanning tree instance to be removed.

Format `no spanning-tree mst instance mstid`

Mode Global Config

spanning-tree mst priority

This command sets the bridge priority for a specific multiple spanning tree instance. The parameter *mstid* is a number that corresponds to the desired existing multiple spanning tree instance. The priority value is a number within a range of 0 to 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 `no spanning-tree mst priority mstid`

Mode Global Config

spanning-tree mst vlan

This command adds an association between a multiple spanning tree instance and one or more VLANs so that the VLAN(s) are no longer associated with the common and internal spanning tree. The parameter *mstid* is a number that corresponds to the desired existing multiple spanning tree instance. The *vlanid* can be specified as a single VLAN, a list, or a range of values. To specify a list of VLANs, enter a list of VLAN IDs, each separated by a comma with no spaces in between. To specify a range of VLANs, separate the beginning and ending VLAN ID with a dash (-). The VLAN IDs may or may not exist in the system.

Format `spanning-tree mst vlan mstid vlanid`

Mode Global Config

no spanning-tree mst vlan

This command removes an association between a multiple spanning tree instance and one or more VLANs so that the VLAN(s) are again associated with the common and internal spanning tree.

Format `no spanning-tree mst vlan` *`mstid vlanid`*

Mode Global Config

spanning-tree port mode

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

Default enabled

Format `spanning-tree port mode`

Mode Interface Config

no spanning-tree port mode

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

Format `no spanning-tree port mode`

Mode Interface Config

spanning-tree port mode all

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

Default enabled

Format `spanning-tree port mode all`

Mode Global Config

no spanning-tree port mode all

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

Format `no spanning-tree port mode all`

Mode Global Config

show spanning-tree

This command displays spanning tree settings for the common and internal spanning tree. The following details are displayed.

Format `show spanning-tree`

Mode
- Privileged EXEC
- User EXEC

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

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

Format `show spanning-tree brief`

Mode
- Privileged EXEC
- User EXEC

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

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`

Mode
- Privileged EXEC
- User EXEC

Term	*Definition*
Hello Time	Admin hello time for this port.
Port Mode	Enabled or disabled.
BPDU Guard Effect	Enabled or disabled.
Root Guard	Enabled or disabled.
Loop Guard	Enabled or disabled.
TCN Guard	Enable or disable the propagation of received topology change notifications and topology changes to other ports.
BPDU Filter Mode	Enabled or disabled.
BPDU Flood Mode	Enabled or disabled.

Term	*Definition*
Auto Edge	To enable or disable the feature that causes a port that has not seen a BPDU for **edge delay** time, to become an edge port and transition to forwarding faster.
Port Up Time Since Counters Last Cleared	Time since port was reset, displayed in days, hours, minutes, and seconds.
STP BPDUs Transmitted	Spanning Tree Protocol Bridge Protocol Data Units sent.
STP BPDUs Received	Spanning Tree Protocol Bridge Protocol Data Units received.
RSTP BPDUs Transmitted	Rapid Spanning Tree Protocol Bridge Protocol Data Units sent.
RSTP BPDUs Received	Rapid Spanning Tree Protocol Bridge Protocol Data Units received.
MSTP BPDUs Transmitted	Multiple Spanning Tree Protocol Bridge Protocol Data Units sent.
MSTP BPDUs Received	Multiple Spanning Tree Protocol Bridge Protocol Data Units received.

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

Term	*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	Indicates whether auto calculation for port path cost is enabled.
Port Path Cost	Configured value of the Internal Port Path Cost parameter.
Designated Root	The Identifier of the designated root for this port.

Term	*Definition*
Root Path Cost	The path cost to get to the root bridge for this instance. The root path cost is zero if the bridge is the root bridge for that instance.
Designated Bridge	Bridge Identifier of the bridge with the Designated Port.
Designated Port Identifier	Port on the Designated Bridge that offers the lowest cost to the LAN.
Loop Inconsistent State	The current loop inconsistent state of this port in this MST instance. When in loop inconsistent state, the port has failed to receive BPDUs while configured with loop guard enabled. Loop inconsistent state maintains the port in a blocking state until a subsequent BPDU is received.
Transitions Into Loop Inconsistent State	The number of times this interface has transitioned into loop inconsistent state.
Transitions Out of Loop Inconsistent State	The number of times this interface has transitioned out of loop inconsistent state.

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

Term	*Definition*
Port Identifier	The port identifier for this port within the CST.
Port Priority	The priority of the port within the CST.
Port Forwarding State	The forwarding state of the port within the CST.
Port Role	The role of the specified interface within the CST.
Auto-Calculate Port Path Cost	Indicates whether auto calculation for port path cost is enabled or not (disabled).
Port Path Cost	The configured path cost for the specified interface.
Auto-Calculate External Port Path Cost	Indicates whether auto calculation for external port path cost is enabled.
External Port Path Cost	The cost to get to the root bridge of the CIST across the boundary of the region. This means that if the port is a boundary port for an MSTP region, then the external path cost is used.
Designated Root	Identifier of the designated root for this port within the CST.
Root Path Cost	The root path cost to the LAN by the port.
Designated Bridge	The bridge containing the designated port.
Designated Port Identifier	Port on the Designated Bridge that offers the lowest cost to the LAN.
Topology Change Acknowledgement	Value of flag in next Configuration Bridge Protocol Data Unit (BPDU) transmission indicating if a topology change is in progress for this port.

Term	*Definition*
Hello Time	The hello time in use for this port.
Edge Port	The configured value indicating if this port is an edge port.
Edge Port Status	The derived value of the edge port status. True if operating as an edge port; false otherwise.
Point To Point MAC Status	Derived value indicating if this port is part of a point to point link.
CST Regional Root	The regional root identifier in use for this port.
CST Internal Root Path Cost	The internal root path cost to the LAN by the designated external port.
Loop Inconsistent State	The current loop inconsistent state of this port in this MST instance. When in loop inconsistent state, the port has failed to receive BPDUs while configured with loop guard enabled. Loop inconsistent state maintains the port in a blocking state until a subsequent BPDU is received.
Transitions Into Loop Inconsistent State	The number of times this interface has transitioned into loop inconsistent state.
Transitions Out of Loop Inconsistent State	The number of times this interface has transitioned out of loop inconsistent state.

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}

Mode
- Privileged EXEC
- User EXEC

Term	*Definition*
MST Instance ID	The MST instance associated with this port.
Interface	*slot/port*
STP Mode	Indicates whether spanning tree is enabled or disabled on the port.
Type	Currently not used.
STP State	The forwarding state of the port in the specified spanning tree instance.
Port Role	The role of the specified port within the spanning tree.
Desc	Indicates whether the port is in loop inconsistent state or not. This field is blank if the loop guard feature is not available.

show spanning-tree mst port summary active

This command displays settings for the ports within the specified multiple spanning tree instance that are active links.

Format `show spanning-tree mst port summary mstid active`

Mode
- Privileged EXEC
- User EXEC

Term	*Definition*
MST Instance ID	The ID of the existing MST instance.
Interface	*slot/port*
STP Mode	Indicates whether spanning tree is enabled or disabled on the port.
Type	Currently not used.
STP State	The forwarding state of the port in the specified spanning tree instance.
Port Role	The role of the specified port within the spanning tree.
Desc	Indicates whether the port is in loop inconsistent state or not. This field is blank if the loop guard feature is not available.

show spanning-tree mst summary

This command displays summary information about all multiple spanning tree instances in the switch. On execution, the following details are displayed.

Format `show spanning-tree mst summary`

Mode
- Privileged EXEC
- User EXEC

Term	*Definition*
MST Instance ID List	List of multiple spanning trees IDs currently configured.
For each MSTID: • Associated FIDs • Associated VLANs	• List of forwarding database identifiers associated with this instance. • List of VLAN IDs associated with this instance.

show spanning-tree summary

This command displays spanning tree settings and parameters for the switch. The following details are displayed on execution of the command.

Format `show spanning-tree summary`

Mode
- Privileged EXEC
- User EXEC

Term	*Definition*
Spanning Tree Adminmode	Enabled or disabled.
Spanning Tree Version	Version of 802.1 currently supported (IEEE 802.1s, IEEE 802.1w, or IEEE 802.1d) based upon the Force Protocol Version parameter.
BPDU Guard Mode	Enabled or disabled.
BPDU Filter Mode	Enabled or disabled.
Configuration Name	Identifier used to identify the configuration currently being used.
Configuration Revision Level	Identifier used to identify the configuration currently being used.
Configuration Digest Key	A generated Key used in the exchange of the BPDUs.
Configuration Format Selector	Specifies the version of the configuration format being used in the exchange of BPDUs. The default value is zero.
MST Instances	List of all multiple spanning tree instances configured on the switch.

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*

Mode
- Privileged EXEC
- User EXEC

Term	*Definition*
VLAN Identifier	The 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.

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` *`1–3965`*

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). The VLAN range is 2–3965.

Format `no vlan` *`2–3965`*

Mode VLAN Config

vlan acceptframe

This command sets the frame acceptance mode on an interface or range of interfaces. For VLAN Only mode, untagged frames or priority frames received on this interface are discarded. For Admit All mode, untagged frames or priority frames received on this interface are accepted and assigned the value of the interface VLAN ID for this port. 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 resets the frame acceptance mode for the interface or range of interfaces to the default value.

Format `no vlan acceptframe`

Mode Interface Config

vlan ingressfilter

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

Default disabled

Format `vlan ingressfilter`

Mode Interface Config

no vlan ingressfilter

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

Format `no vlan ingressfilter`

Mode Interface Config

vlan makestatic

This command changes a dynamically created VLAN (created by GVRP registration) to a static VLAN (one that is permanently configured and defined). The ID is a valid VLAN identification number. VLAN range is 2–3965.

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 1–3965.

Default
- VLAN ID 1 - default
- other VLANS - blank string

Format `vlan name 1–3965 name`

Mode VLAN Config

no vlan name

This command sets the name of a VLAN to a blank string.

Format `no vlan name 1–3965`

Mode VLAN Config

vlan participation

This command configures the degree of participation for a specific interface or range of interfaces in a VLAN. The ID is a valid VLAN identification number, and the interface is a valid interface number .

Format `vlan participation {exclude | include | auto} 1–3965`

Mode Interface Config

Participation options are:

Options	*Definition*
include	The interface is always a member of this VLAN. This is equivalent to registration fixed.
exclude	The interface is never a member of this VLAN. This is equivalent to registration forbidden.
auto	The interface is dynamically registered in this VLAN by GVRP and will not participate in this VLAN unless a join request is received on this interface. This is equivalent to registration normal.

vlan participation all

This command configures the degree of participation for all interfaces in a VLAN. The ID is a valid VLAN identification number.

Format `vlan participation all {exclude | include | auto} 1–3965`

Mode Global Config

You can use the following participation options:

Participation Options	*Definition*
include	The interface is always a member of this VLAN. This is equivalent to registration fixed.
exclude	The interface is never a member of this VLAN. This is equivalent to registration forbidden.
auto	The interface is dynamically registered in this VLAN by GVRP. The interface will not participate in this VLAN unless a join request is received on this interface. This is equivalent to registration normal.

vlan port acceptframe all

This command sets the frame acceptance mode for all interfaces.

Default all

Format `vlan port acceptframe all {vlanonly | all}`

Mode Global Config

The modes are defined as follows:

Mode	*Definition*
VLAN Only mode	Untagged frames or priority frames received on this interface are discarded.
Admit All mode	Untagged frames or priority frames received on this interface are accepted and assigned the value of the interface VLAN ID for this port.

With either option, VLAN tagged frames are forwarded in accordance with the IEEE 802.1Q VLAN Specification.

no vlan port acceptframe all

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

Format `no vlan port acceptframe all`

Mode Global Config

vlan port ingressfilter all

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

Default disabled

Format `vlan port ingressfilter all`

Mode Global Config

no vlan port ingressfilter all

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

Format `no vlan port ingressfilter all`

Mode Global Config

vlan port pvid all

This command changes the VLAN ID for all interface.

Default 1

Format `vlan port pvid all` *`1–3965`*

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` *`1–3965`*

Mode Global Config

no vlan port tagging all

This command configures the tagging behavior for all interfaces in a VLAN to disabled. If tagging is disabled, traffic is transmitted as untagged frames. The ID is a valid VLAN identification number.

Format `no vlan port tagging all`

Mode Global Config

vlan protocol group

This command adds protocol-based VLAN groups to the system. The *groupid* is a unique number from 1–128 that is used to identify the group in subsequent commands.

Format `vlan protocol group` *groupid*

Mode Global Config

vlan protocol group name

This command assigns a name to a protocol-based VLAN groups. The *groupname* variable can be a character string of 0 to 16 characters.

Format `vlan protocol group name` *groupid groupname*

Mode Global Config

no vlan protocol group name

This command removes the name from the group identified by *groupid*.

Format `no vlan protocol group name` *groupid*

Mode Global Config

vlan protocol group add protocol

This command adds the `protocol` to the protocol-based VLAN identified by *groupid*. A group may have more than one protocol associated with it. Each interface and protocol combination can only be associated with one group. If adding a protocol to a group causes any conflicts with interfaces currently associated with the group, this command fails and the protocol is not added to the group. The possible values for *protocol-list* includes the keywords `ip, arp, and ipx` and hexadecimal or decimal values ranging from 0x0600 (1536) to 0xFFFF (65535). The protocol list can accept up to 16 protocols separated by a comma.

Default none

Format `vlan protocol group add protocol` *groupid ethertype protocol-list*

Mode Global Config

no vlan protocol group add protocol

This command removes the protocols specified in the *protocol-list* from this protocol-based VLAN group that is identified by this *groupid*.

Format no vlan protocol group add protocol *groupid ethertype protocol-list*

Mode Global Config

protocol group

This command attaches a *vlanid* to the protocol-based VLAN identified by *groupid*. A group may only be associated with one VLAN at a time, however the VLAN association can be changed.

Default none

Format protocol group *groupid vlanid*

Mode VLAN Config

no protocol group

This command removes the *vlanid* from this protocol-based VLAN group that is identified by this *groupid*.

Format no protocol group *groupid vlanid*

Mode VLAN Config

protocol vlan group

This command adds a physical interface or a range of interfaces to the protocol-based VLAN identified by *groupid*. You can associate multiple interfaces with a group, but you can only associate each interface and protocol combination with one group. If adding an interface to a group causes any conflicts with protocols currently associated with the group, this command fails and the interface(s) are not added to the group.

Default none

Format protocol vlan group *groupid*

Mode Interface Config

no protocol vlan group

This command removes the interface from this protocol-based VLAN group that is identified by this *groupid*.

Format no protocol vlan group *groupid*

Mode Interface Config

protocol vlan group all

This command adds all physical interfaces to the protocol-based VLAN identified by *groupid*. You can associate multiple interfaces with a group, but you can only associate each interface and protocol combination with one group. If adding an interface to a group causes any conflicts with protocols currently associated with the group, this command will fail and the interface(s) will not be added to the group.

Default none

Format `protocol vlan group all groupid`

Mode Global Config

no protocol vlan group all

This command removes all interfaces from this protocol-based VLAN group that is identified by this *groupid*.

Format `no protocol vlan group all groupid`

Mode Global Config

show port protocol

This command displays the Protocol-Based VLAN information for either the entire system, or for the indicated group.

Format `show port protocol {groupid | all}`

Mode Privileged EXEC

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

vlan pvid

This command changes the VLAN ID on an interface or range of interfaces.

Default 1

Format `vlan pvid 1–3965`

Mode Interface Config
Interface Range Config

no vlan pvid

This command sets the VLAN ID on an interface or range of interfaces to 1.

Format `no vlan pvid`

Mode Interface Config

vlan tagging

This command configures the tagging behavior for a specific interface or range of interfaces in a VLAN to enabled. If tagging is enabled, traffic is transmitted as tagged frames. If tagging is disabled, traffic is transmitted as untagged frames. The ID is a valid VLAN identification number.

Format `vlan tagging` *`1—3965`*

Mode
- Interface Config

no vlan tagging

This command configures the tagging behavior for a specific interface or range of interfaces in a VLAN to disabled. If tagging is disabled, traffic is transmitted as untagged frames. The ID is a valid VLAN identification number.

Format `no vlan tagging` *`1—3965`*

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*

Mode
- Privileged EXEC
- User EXEC

Term	*Definition*
VLAN ID	There is a VLAN Identifier (VID) associated with each VLAN. The range of the VLAN ID is 1 to 3965.
VLAN Name	A string associated with this VLAN as a convenience. It can be up to 32 alphanumeric characters long, including blanks. The default is blank. VLAN ID 1 always has a name of *Default*. This field is optional.
VLAN Type	Type of VLAN, which can be Default (VLAN ID = 1) or static (one that is configured and permanently defined), or Dynamic. A dynamic VLAN can be created by GVRP registration or during the 802.1X authentication process (DOT1X) if a RADIUS-assigned VLAN does not exist on the switch.
Interface	slot/port It is possible to set the parameters for all ports by using the selectors on the top line.
Current	The degree of participation of this port in this VLAN. The permissible values are: • **Include** - This port is always a member of this VLAN. This is equivalent to registration fixed in the IEEE 802.1Q standard. • **Exclude** - This port is never a member of this VLAN. This is equivalent to registration forbidden in the IEEE 802.1Q standard. • **Autodetect** - To allow the port to be dynamically registered in this VLAN via GVRP. The port will not participate in this VLAN unless a join request is received on this port. This is equivalent to registration normal in the IEEE 802.1Q standard.

Term	*Definition*
Configured	The configured degree of participation of this port in this VLAN. The permissible values are: • **Include** - This port is always a member of this VLAN. This is equivalent to registration fixed in the IEEE 802.1Q standard. • **Exclude** - This port is never a member of this VLAN. This is equivalent to registration forbidden in the IEEE 802.1Q standard. • **Autodetect** - To allow the port to be dynamically registered in this VLAN via GVRP. The port will not participate in this VLAN unless a join request is received on this port. This is equivalent to registration normal in the IEEE 802.1Q standard.
Tagging	The tagging behavior for this port in this VLAN. • **Tagged** - Transmit traffic for this VLAN as tagged frames. • **Untagged** - Transmit traffic for this VLAN as untagged frames.

show vlan internal usage

This command displays information about the VLAN ID allocation on the switch.

Format `show vlan internal usage`

Mode
- Privileged EXEC
- User EXEC

Term	*Definition*
Base VLAN ID	Identifies the base VLAN ID for Internal allocation of VLANs to the routing interface.
Allocation policy	Identifies whether the system allocates VLAN IDs in ascending or descending order.

show vlan brief

This command displays a list of all configured VLANs.

Format `show vlan brief`

Mode
- Privileged EXEC
- User EXEC

Term	*Definition*
VLAN ID	There is a VLAN Identifier (vlanid) associated with each VLAN. The range of the VLAN ID is 1 to 3965.
VLAN Name	A string associated with this VLAN as a convenience. It can be up to 32 alphanumeric characters long, including blanks. The default is blank. VLAN ID 1 always has a name of *Default*. This field is optional.
VLAN Type	Type of VLAN, which can be Default (VLAN ID = 1) or static (one that is configured and permanently defined), or a Dynamic (one that is created by GVRP registration).

show vlan port

This command displays VLAN port information.

Format `show vlan port {slot/port | all}`

Mode
- Privileged EXEC
- User EXEC

Term	*Definition*
Interface	slot/port It is possible to set the parameters for all ports by using the selectors on the top line.
Port VLAN ID	The VLAN ID that this port will assign to untagged frames or priority tagged frames received on this port. The value must be for an existing VLAN. The factory default is 1.
Acceptable Frame Types	The types of frames that may be received on this port. The options are 'VLAN only' and 'Admit All'. When set to 'VLAN only', untagged frames or priority tagged frames received on this port are discarded. When set to 'Admit All', untagged frames or priority tagged frames received on this port are accepted and assigned the value of the Port VLAN ID for this port. With either option, VLAN tagged frames are forwarded in accordance to the 802.1Q VLAN specification.
Ingress Filtering	May be enabled or disabled. When enabled, the frame is discarded if this port is not a member of the VLAN with which this frame is associated. In a tagged frame, the VLAN is identified by the VLAN ID in the tag. In an untagged frame, the VLAN is the Port VLAN ID specified for the port that received this frame. When disabled, all frames are forwarded 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

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

show vlan association mac

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

Format `show vlan association mac [macaddr]`

Mode Privileged EXEC

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

Double VLAN Commands

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

dvlan-tunnel ethertype (Global Config)

This command configures the ethertype for all interfaces. The two-byte hex EtherType is used as the first 16 bits of the DVLAN tag. The ethertype may have the values of `802.1Q, vman, or custom`. If the ethertype has an optional value of `custom`, then it is a custom tunnel value, and ethertype must be set to a value in the range of 0 to 65535.

Default vman

Format `dvlan-tunnel ethertype {802.1Q | vman | custom 0–65535}`

Mode Global Config

Parameter	*Description*
802.1Q	Configure the ethertype as 0x8100.
custom	Configure the value of the custom tag in the range from 0 to 65535.
vman	Represents the commonly used value of 0x88A8.

dvlan-tunnel ethertype (Interface Config)

Use this command to associate globally defined TPID(s) to an interface or range of interfaces. If the TPID is not yet defined, the system returns an error message to the user.

Format `dvlan-tunnel ethertype {802.1Q | vman | custom 0–65535}`

Mode Interface Config

Parameter	*Description*
802.1Q	Configure the ethertype as 0x8100.
custom	Configure the value of the custom tag in the range from 0 to 65535.
vman	Represents the commonly used value of 0x88A8.

no dvlan-tunnel ethertype (Interface Config)

Use the `no` form of the command to disassociate globally defined TPID(s) to an interface.

Format `no dvlan-tunnel ethertype {802.1Q | vman | custom 0–65535}`

Mode Interface Config

dvlan-tunnel ethertype default-tpid

Use this command to create a new TPID and associate it with the next available TPID register. If no TPID registers are empty, the system returns an error to the user. Specifying the optional keyword `[default–tpid]` forces the TPID value to be configured as the default TPID at index 0.

Format `dvlan-tunnel ethertype {802.1Q | vman | custom 0–65535} [default-tpid]`

Mode Global Config

Parameter	*Description*
802.1Q	Configure the ethertype as 0x8100.
custom	Configure the value of the custom tag in the range from 0 to 65535.
vman	Represents the commonly used value of 0x88A8.

no dvlan-tunnel ethertype default–tpid

Use the `no` form of the command to set the TPID register to 0. (At initialization, all TPID registers will be set to their default values.)

Format `no dvlan-tunnel ethertype {802.1Q | vman | custom 0–65535} [default-tpid]`

Mode Global Config

mode dot1q-tunnel

This command is used to enable Double VLAN Tunneling on the specified interface.

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

no mode dot1q-tunnel

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

Format	`no mode dot1q-tunnel`
Mode	Interface Config

mode dvlan-tunnel

Use this command to enable Double VLAN Tunneling on the specified interface.

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

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

no mode dvlan-tunnel

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

Format	`no mode dvlan-tunnel`
Mode	Interface Config

show dot1q-tunnel

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

Format `show dot1q-tunnel [interface {slot/port | all}]`

Mode
- Privileged EXEC
- User EXEC

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

Mode
- Privileged EXEC
- User EXEC

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

Example: The following shows examples of the CLI display output for the commands.

```
(Routing) #show dvlan-tunnel

TPIDs Configured.............................. 0x88a8
Default TPID.................................. 0x88a8
```

```
Interfaces Enabled for DVLAN Tunneling......... None

(Routing) #

(switch)#show dvlan-tunnel interface 1/0/1

Interface Mode    EtherType
--------- ------- ------------
1/0/1     Disable 0x88a8
```

Voice VLAN Commands

This section describes the commands you use for Voice VLAN. Voice VLAN enables switch ports to carry voice traffic with defined priority so as to enable separation of voice and data traffic coming onto the port. The benefits of using Voice VLAN is to ensure that the sound quality of an IP phone could be safeguarded from deteriorating when the data traffic on the port is high.

Also the inherent isolation provided by VLANs ensures that inter-VLAN traffic is under management control and that network- attached clients cannot initiate a direct attack on voice components. QoS-based on IEEE 802.1P class of service (CoS) uses classification and scheduling to sent network traffic from the switch in a predictable manner. The system uses the source MAC of the traffic traveling through the port to identify the IP phone data flow.

voice vlan (Global Config)

Use this command to enable the Voice VLAN capability on the switch.

Default	disabled
Format	`voice vlan`
Mode	Global Config

no voice vlan (Global Config)

Use this command to disable the Voice VLAN capability on the switch.

Format	`no voice vlan`
Mode	Global Config

voice vlan (Interface Config)

Use this command to enable the Voice VLAN capability on the interface or range of interfaces.

Default disabled

Format `voice vlan {vlanid id | dot1p priority | none | untagged}`

Mode Interface Config

You can configure Voice VLAN in one of four different ways:

Parameter	*Description*
vlan-id	Configure the IP phone to forward all voice traffic through the specified VLAN. Valid VLAN ID's are from 1 to 4093 (the max supported by the platform).
dot1p	Configure the IP phone to use 802.1p priority tagging for voice traffic and to use the default native VLAN (VLAN 0) to carry all traffic. Valid *priority* range is 0 to 7.
none	Allow the IP phone to use its own configuration to send untagged voice traffic.
untagged	Configure the phone to send untagged voice traffic.

no voice vlan (Interface Config)

Use this command to disable the Voice VLAN capability on the interface.

Format `no voice vlan`

Mode Interface Config

voice vlan data priority

Use this command to either trust or untrust the data traffic arriving on the Voice VLAN interface or range of interfaces being configured.

Default trust

Format `voice vlan data priority {untrust | trust}`

Mode Interface Config

show voice vlan

Format `show voice vlan [interface {unit/slot/port | all}]`

Mode Privileged EXEC

When the `interface` parameter is not specified, only the global mode of the Voice VLAN is displayed.

Term	*Definition*
Administrative Mode	The Global Voice VLAN mode.

When the `interface` is specified:

Term	*Definition*
Voice VLAN Mode	The admin mode of the Voice VLAN on the interface.
Voice VLAN ID	The Voice VLAN ID
Voice VLAN Priority	The do1p priority for the Voice VLAN on the port.
Voice VLAN Untagged	The tagging option for the Voice VLAN traffic.
Voice VLAN CoS Override	The Override option for the voice traffic arriving on the port.
Voice VLAN Status	The operational status of Voice VLAN on the port.

Provisioning (IEEE 802.1p) Commands

This section describes the commands you use to configure provisioning (IEEE 802.1p,) which allows you to prioritize ports.

vlan port priority all

This command configures the port priority assigned for untagged packets for all ports presently plugged into the device. The range for the priority is 0–7. Any subsequent per port configuration will override this configuration setting.

Format `vlan port priority all` *priority*

Mode Global Config

vlan priority

This command configures the default 802.1p port priority assigned for untagged packets for a specific interface. The range for the priority is 0–7.

Default 0

Format `vlan priority` *priority*

Mode Interface Config

Priority-Based Flow Control Commands

Ordinarily, when flow control is enabled on a physical link, it applies to all traffic on the link. When congestion occurs, the hardware sends pause frames that temporarily suspend traffic flow. Pausing traffic helps prevent buffer overflow and dropped frames.

Priority-based flow control provides a way to distinguish which traffic on physical link is paused when congestion occurs, based on the priority of the traffic. An interface can be configured to pause only high priority (i.e., loss-sensitive) traffic when necessary prevent dropped frames, while allowing traffic that has greater loss tolerance to continue to flow on the interface.

Priorities are differentiated by the priority field of the IEEE 802.1Q VLAN header, which identifies an IEEE 802.1p priority value. In DWS-4000, these priority values must be mapped to internal class-of-service (CoS) values.

To enable priority-based flow control for a particular CoS value on an interface:

1. Ensure that VLAN tagging is enabled on the interface so that the 802.1p priority values are carried through the network (see "Provisioning (IEEE 802.1p) Commands" on page 253).
2. Ensure that 802.1p priority values are mapped to DWS-4000 CoS values (see "classofservice dot1p-mapping" on page 789).
3. Use the `datacenter-bridging priority-flow-control mode on` command to enable priority-based flow control on the interface.
4. Use the `datacenter-bridging priority-flow-control priority` command to specify the CoS values that should be paused (no-drop) due to greater loss sensitivity. Unless configured as *no-drop*, all CoS priorities are considered non-pausable (drop) when priority-based flow control is enabled.

When priority-flow-control is disabled, the interface defaults to the IEEE 802.3x flow control setting for the interface. When priority-based flow control is enabled, the interface will not pause any CoS unless there is at least one no-drop priority.

datacenter-bridging priority-flow-control mode on

Use this command to enable priority-based flow control on an interface.

Default	Disabled
Format	`datacenter-bridging priority-flow-control mode on`
Mode	Interface Config

Example: The following example enables priority flow control on interface 1/0/1.

```
console(1/0/1)# datacenter-bridging priority-flow-control mode on
```

no datacenter-bridging priority-flow-control mode

Use this command to disable priority flow control on an interface.

Format `no datacenter-bridging priority-flow-control`

Mode Interface Config

datacenter-bridging priority-flow-control priority

Use this command to specify the priority group(s) that should be paused when necessary to prevent dropped frames; i.e., the group to receive priority flow control.

This configuration has no effect on interfaces not enabled for priority flow control. VLAN tagging must be enabled to carry the 802.1p value through the network. Additionally, the mapping of class-of-service levels to 802.1p priority values to must be set to one-to-one (see command "classofservice dot1p-mapping" on page 789).

Default drop

Format `datacenter-bridging priority-flow-control priority` *`priority-list`* `{drop | no-drop}`

Mode Interface Config

Example: The following commands maps 802.1p priority values to internal class-of-service values, enables VLAN tagging on interface 1/0/1, and then enables priority-based flow control for priority 5 traffic:

```
(Switch) #configure
classofservice dot1p-mapping 0 0
classofservice dot1p-mapping 1 1
classofservice dot1p-mapping 2 2
classofservice dot1p-mapping 3 3
classofservice dot1p-mapping 4 4
classofservice dot1p-mapping 5 5
classofservice dot1p-mapping 6 6
classofservice dot1p-mapping 7 7
interface 1/0/1
vlan tagging 1
datacenter-bridging priority-flow-control mode on
datacenter-bridging priority-flow-control priority 5 no-drop
exit
exit
```

show datacenter-bridging priority-flow-control

This command displays a summary of the priority flow control configuration for a specified interface or all interfaces.

Format `show datacenter-bridging priority-flow-control [interface interface]`

Mode Privileged EXEC

Example: The following example shows the output of the command:

```
(Switch) #show datacenter-bridging priority-flow-control

Port       Drop          No-Drop          State
           Priorities    Priorities
----       ----------    ----------       -----
1/0/1      1-4,7         5,6              Enabled
1/0/2      1-4,6-7       5                Enabled
….
1/0/48     1-4,7         5,6              Enabled
```

show interfaces datacenter bridging

This command displays the priority-based flow control configuration, status, and counters for a specified interface or all interfaces.

Format `show interface datacenter-bridging`

Mode Privileged EXEC

Example: The following example shows

```
(Switch) #show interface ethernet 1/0/1 datacenter-bridging

Port       Drop          No-Drop       State
           Priorities    Priorities
----       ----------    ----------    -----
1/0/1      1-4,7         5,6           Enabled

Priority       Received PFC frames
0              0
1              0
2              0
3              0
4              0

5              0
6              0
7              0

Received PFC Frames:      0
Transmit PFC Frames:      0
```

clear priority-flow-control statistics

Use this command to reset the PFC counters to zero. Include the slot/port to clear the PFC statistics on a specific port.

Format `clear priority-flow-control statistics [slot/port]`

Mode Privileged EXEC

Protected Ports Commands

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

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

switchport protected (Global Config)

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

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

Default unprotected

Format `switchport protected` *groupid* `name` *name*

Mode Global Config

no switchport protected (Global Config)

Use this command to remove a protected port group. The *groupid* parameter identifies the set of protected ports. The `name` keyword specifies the name to remove from the group.

Format `no switchport protected` *groupid* `name`

Mode Global Config

switchport protected (Interface Config)

Use this command to add an interface to a protected port group. The *groupid* parameter identifies the set of protected ports to which this interface is assigned. You can only configure an interface as protected in one group.

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

Default unprotected

Format `switchport protected groupid`

Mode Interface Config

no switchport protected (Interface Config)

Use this command to configure a port as unprotected. The *groupid* parameter identifies the set of protected ports to which this interface is assigned.

Format `no switchport protected groupid`

Mode Interface Config

show switchport protected

This command displays the status of all the interfaces, including protected and unprotected interfaces.

Format `show switchport protected groupid`

Mode
- Privileged EXEC
- User EXEC

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

show interfaces switchport

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

Format `show interfaces switchport slot/port groupid`

Mode
- Privileged EXEC
- User EXEC

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

GARP Commands

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

set garp timer join

This command sets the GVRP join time per GARP for one interface, a range of interfaces, or all interfaces. Join time is the interval between the transmission of GARP Protocol Data Units (PDUs) registering (or 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`

Mode
- Interface Config
- Global Config

no set garp timer join

This command sets the GVRP join time to the default and only has an effect when GVRP is enabled.

Format `no set garp timer join`

Mode
- Interface Config
- Global Config

set garp timer leave

This command sets the GVRP leave time for one interface, a range of interfaces, or all interfaces or all ports and only has an effect when GVRP is enabled. Leave time is the time to wait after receiving an unregister request for a VLAN or a multicast group before deleting the VLAN entry. This can be considered a buffer time for another station to assert registration for the same attribute in order to maintain uninterrupted service. The leave time is 20 to 600 (centiseconds). The value 60 centiseconds is 0.6 seconds. The leave time must be greater than or equal to three times the join time.

Default 60

Format `set garp timer leave` *`20–600`*

Mode
- Interface Config
- Global Config

no set garp timer leave

This command sets the GVRP leave time on all ports or a single port to the default and only has an effect when GVRP is enabled.

Format `no set garp timer leave`

Mode
- Interface Config
- Global Config

set garp timer leaveall

This command sets how frequently Leave All PDUs are generated. A Leave All PDU indicates that all registrations will be unregistered. Participants would need to rejoin in order to maintain registration. The value applies per port and per GARP participation. The time may range from 200 to 6000 (centiseconds). The value 1000 centiseconds is 10 seconds. You can use this command on all ports (Global Config mode), or on a single port or a range of ports (Interface Config mode) and it only has an effect only when GVRP is enabled. The leave all time must be greater than the leave time.

Default 1000

Format `set garp timer leaveall` *`200–6000`*

Mode
- Interface Config
- Global Config

no set garp timer leaveall

This command sets how frequently Leave All PDUs are generated the default and only has an effect when GVRP is enabled.

Format `no set garp timer leaveall`

Mode
- Interface Config
- Global Config

show garp

This command displays GARP information.

Format `show garp`

Mode
- Privileged EXEC
- User EXEC

Term	*Definition*
GMRP Admin Mode	The administrative mode of GARP Multicast Registration Protocol (GMRP) for the system.
GVRP Admin Mode	The administrative mode of GARP VLAN Registration Protocol (GVRP) for the system.

GVRP Commands

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

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

set gvrp adminmode

This command enables GVRP on the system.

Default disabled

Format `set gvrp adminmode`

Mode Privileged EXEC

no set gvrp adminmode

This command disables GVRP.

Format `no set gvrp adminmode`

Mode Privileged EXEC

set gvrp interfacemode

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

Default disabled

Format `set gvrp interfacemode`

Mode
- Interface Config
- Interface Range
- Global Config

no set gvrp interfacemode

This command disables GVRP on a single port (Interface Config mode) or all ports (Global Config mode). If GVRP is disabled, Join Time, Leave Time and Leave All Time have no effect.

Format `no set gvrp interfacemode`

Mode
- Interface Config
- Global Config

show gvrp configuration

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

Format `show gvrp configuration {slot/port | all}`

Mode
- Privileged EXEC
- User EXEC

Term	*Definition*
Interface	*slot/port*
Join Timer	The interval between the transmission of GARP PDUs registering (or 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	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).

Term	*Definition*
LeaveAll Timer	This Leave All Time controls how frequently LeaveAll PDUs are generated. A LeaveAll PDU indicates that all registrations will shortly be deregistered. Participants will need to rejoin in order to maintain registration. There is an instance of this timer on a per-Port, per-GARP participant basis. The Leave All Period Timer is set to a random value in the range of LeaveAllTime to 1.5*LeaveAllTime. Permissible values are 200 to 6000 centiseconds (2 to 60 seconds). The factory default is 1000 centiseconds (10 seconds).
Port GMRP Mode	The GMRP administrative mode for the port, which is enabled or disabled (default). If this parameter is disabled, Join Time, Leave Time and Leave All Time have no effect.

GMRP Commands

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

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

set gmrp adminmode

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

Default disabled

Format `set gmrp adminmode`

Mode Privileged EXEC

no set gmrp adminmode

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

Format `no set gmrp adminmode`

Mode Privileged EXEC

set gmrp interfacemode

This command enables GARP Multicast Registration Protocol on a single interface (Interface Config mode), a range of interfaces, or all interfaces (Global Config mode). If an interface which has GARP enabled is enabled for routing or is enlisted as a member of a port-channel (LAG), GARP functionality is disabled on that interface. GARP functionality is subsequently re-enabled if routing is disabled and port-channel (LAG) membership is removed from an interface that has GARP enabled.

Default disabled

Format `set gmrp interfacemode`

Mode
- Interface Config
- Global Config

no set gmrp interfacemode

This command disables GARP Multicast Registration Protocol on a single interface or all interfaces. If an interface which has GARP enabled is enabled for routing or is enlisted as a member of a port-channel (LAG), GARP functionality is disabled. GARP functionality is subsequently re-enabled if routing is disabled and port-channel (LAG) membership is removed from an interface that has GARP enabled.

Format `no set gmrp interfacemode`

Mode
- Interface Config
- Global Config

show gmrp configuration

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

Format `show gmrp configuration {slot/port | all}`

Mode
- Privileged EXEC
- User EXEC

Term	*Definition*
Interface	The slot/port of the interface that this row in the table describes.
Join Timer	The interval between the transmission of GARP PDUs registering (or re-registering) membership for an attribute. Current attributes are a VLAN or multicast group. There is an instance of this timer on a per-port, per-GARP participant basis. Permissible values are 10 to 100 centiseconds (0.1 to 1.0 seconds). The factory default is 20 centiseconds (0.2 seconds). The finest granularity of specification is 1 centisecond (0.01 seconds).
Leave Timer	The period of time to wait after receiving an unregister request for an attribute before deleting the attribute. Current attributes are a VLAN or multicast group. This may be considered a buffer time for another station to assert registration for the same attribute in order to maintain uninterrupted service. There is an instance of this timer on a per-Port, per-GARP participant basis. Permissible values are 20 to 600 centiseconds (0.2 to 6.0 seconds). The factory default is 60 centiseconds (0.6 seconds).

Term	*Definition*
LeaveAll Timer	This Leave All Time controls how frequently LeaveAll PDUs are generated. A LeaveAll PDU indicates that all registrations will shortly be deregistered. Participants will need to rejoin in order to maintain registration. There is an instance of this timer on a per-Port, per-GARP participant basis. The Leave All Period Timer is set to a random value in the range of LeaveAllTime to 1.5*LeaveAllTime. Permissible values are 200 to 6000 centiseconds (2 to 60 seconds). The factory default is 1000 centiseconds (10 seconds).
Port GMRP Mode	The GMRP administrative mode for the port. It may be enabled or disabled. If this parameter is disabled, Join Time, Leave Time and Leave All Time have no effect.

show mac-address-table gmrp

This command displays the GMRP entries in the Multicast Forwarding Database (MFDB) table.

Format `show mac-address-table gmrp`

Mode Privileged EXEC

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

Port-Based Network Access Control Commands

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

aaa authentication dot1x default

Use this command to configure the authentication method for port-based access to the switch. The additional methods of authentication are used only if the previous method returns an error, not if there is an authentication failure. The possible methods are as follows:

- ias. Uses the internal authentication server users database for authentication.
- local. Uses the local username database for authentication.
- none. Uses no authentication.
- radius. Uses the list of all RADIUS servers for authentication.

Format `aaa authentication dot1x default` *`method1 [method2...]`*

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 dot1x authentication-history

This command clears the authentication history table captured during successful and unsuccessful authentication on all interface or the specified interface.

Format `clear dot1x authentication-history [slot/port]`

Mode Privileged EXEC

clear radius statistics

This command is used to clear all RADIUS statistics.

Format `clear radius statistics`

Mode Privileged EXEC

dot1x dynamic-vlan enable

Use this command to enable the switch to create VLANs dynamically when a RADIUS-assigned VLAN does not exist in the switch.

Default Disabled

Format `dot1x dynamic-vlan enable`

Mode Global Config

no dot1x dynamic-vlan enable

Use this command to prevent the switch from creating VLANs when a RADIUS-assigned VLAN does not exist in the switch.

Format `no dot1x dynamic-vlan enable`

Mode Global Config

dot1x guest-vlan

This command configures VLAN as guest vlan on an interface or a range of interfaces. The command specifies an active VLAN as an IEEE 802.1X guest VLAN. The range is 1 to the maximum VLAN ID supported by the platform.

Default disabled

Format `dot1x guest-vlan` *`vlan-id`*

Mode Interface Config

no dot1x guest-vlan

This command disables Guest VLAN on the interface.

Default disabled

Format `no dot1x guest-vlan`

Mode Interface Config

dot1x initialize

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

Format `dot1x initialize slot/port`

Mode Privileged EXEC

dot1x max-req

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

Default 2

Format `dot1x max-req` *count*

Mode Interface Config

no dot1x max-req

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

Format `no dot1x max-req`

Mode Interface Config

dot1x max-users

Use this command to set the maximum number of clients supported on an interface or range of interfaces when MAC-based dot1x authentication is enabled on the port. The maximum users supported per port is dependent on the product. The *count* value is in the range 1 - 16.

Default 16

Format `dot1x max-users` *count*

Mode Interface Config

no dot1x max-users

This command resets the maximum number of clients allowed per port to its default value.

Format `no dot1x max-req`

Mode Interface Config

dot1x port-control

This command sets the authentication mode to use on the specified interface or range of interfaces. Use the `force-unauthorized` parameter to specify that the authenticator PAE unconditionally sets the controlled port to unauthorized. Use the `force-authorized` parameter to specify that the authenticator PAE unconditionally sets the controlled port to authorized. Use the `auto` parameter to specify that the authenticator PAE sets the controlled port mode to reflect the outcome of the authentication exchanges between the supplicant, authenticator and the authentication server. If the `mac-based` option is specified, then MAC-based dot1x authentication is enabled on the port.

Default auto

Format `dot1x port-control {force-unauthorized | force-authorized | auto | mac-based}`

Mode Interface Config

no dot1x port-control

This command sets the 802.1X port control mode on the specified port to the default value.

Format `no dot1x port-control`

Mode Interface Config

dot1x port-control all

This command sets the authentication mode to use on all ports. Select `force-unauthorized` to specify that the authenticator PAE unconditionally sets the controlled port to unauthorized. Select `force-authorized` to specify that the authenticator PAE unconditionally sets the controlled port to authorized. Select `auto` to specify that the authenticator PAE sets the controlled port mode to reflect the outcome of the authentication exchanges between the supplicant, authenticator and the authentication server. If the `mac-based` option is specified, then MAC-based dot1x authentication is enabled on the port.

Default auto

Format `dot1x port-control all {force-unauthorized | force-authorized | auto | mac-based}`

Mode Global Config

no dot1x port-control all

This command sets the authentication mode on all ports to the default value.

Format `no dot1x port-control all`

Mode Global Config

dot1x re-authenticate

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

Format `dot1x re-authenticate slot/port`

Mode Privileged EXEC

dot1x re-authentication

This command enables re-authentication of the supplicant for the specified interface or range of interfaces.

Default disabled

Format `dot1x re-authentication`

Mode Interface Config

no dot1x re-authentication

This command disables 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 system-auth-control monitor

Use this command to enable the 802.1X monitor mode on the switch. The purpose of Monitor mode is to help troubleshoot port-based authentication configuration issues without disrupting network access for hosts connected to the switch. In Monitor mode, a host is granted network access to an 802.1X-enabled port even if it fails the authentication process. The results of the process are logged for diagnostic purposes.

Default disabled

Format `dot1x system-auth-control monitor`

Mode Global Config

no dot1x system-auth-control monitor

This command disables the 802.1X Monitor mode on the switch.

Format `no dot1x system-auth-control monitor`

Mode Global Config

dot1x timeout

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

Tokens	*Definition*
guest-vlan-period	The time, in seconds, for which the authenticator waits to see if any EAPOL packets are received on a port before authorizing the port and placing the port in the guest vlan (if configured). The guest vlan timer is only relevant when guest vlan has been configured on that specific port.
reauth-period	The value, in seconds, of the timer used by the authenticator state machine on this port to determine when re-authentication of the supplicant takes place. The reauth-period must be a value in the range 1 - 65535.
quiet-period	The value, in seconds, of the timer used by the authenticator state machine on this port to define periods of time in which it will not attempt to acquire a supplicant. The quiet-period must be a value in the range 0 - 65535.
tx-period	The value, in seconds, of the timer used by the authenticator state machine on this port to determine when to send an EAPOL EAP Request/Identity frame to the supplicant. The quiet-period must be a value in the range 1 - 65535.
supp-timeout	The value, in seconds, of the timer used by the authenticator state machine on this port to timeout the supplicant. The supp-timeout must be a value in the range 1 - 65535.
server-timeout	The value, in seconds, of the timer used by the authenticator state machine on this port to timeout the authentication server. The supp-timeout must be a value in the range 1 - 65535.

Default
- guest-vlan-period: 90 seconds
- reauth-period: 3600 seconds
- quiet-period: 60 seconds
- tx-period: 30 seconds
- supp-timeout: 30 seconds
- server-timeout: 30 seconds

Format `dot1x timeout {{guest-vlan-period` *`seconds`*`} |{reauth-period` *`seconds`*`} | {quiet-period` *`seconds`*`} | {tx-period` *`seconds`*`} | {supp-timeout` *`seconds`*`} | {server-timeout` *`seconds`*`}}`

Mode Interface Config

no dot1x timeout

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

Format `no dot1x timeout {guest-vlan-period | reauth-period | quiet-period | tx-period | supp-timeout | server-timeout}`

Mode Interface Config

dot1x unauthenticated-vlan

Use this command to configure the unauthenticated VLAN associated with the specified interface or range of interfaces. The unauthenticated VLAN ID can be a valid VLAN ID from 0-Maximum supported VLAN ID (3965 for DWS-4000). The unauthenticated VLAN must be statically configured in the VLAN database to be operational. By default, the unauthenticated VLAN is 0, i.e. invalid and not operational.

Default 0

Format `dot1x unauthenticated-vlan` *`vlan id`*

Mode Interface Config

no dot1x unauthenticated-vlan

This command resets the unauthenticated-vlan associated with the port to its default value.

Format `no dot1x unauthenticated-vlan`

Mode Interface Config

dot1x user

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

Format `dot1x user` *`user`* `{slot/port | all}`

Mode Global Config

no dot1x user

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

Format `no dot1x user user {slot/port | all}`

Mode Global Config

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

Term	*Definition*
Authentication Login List	The authentication login listname.
Method 1	The first method in the specified authentication login list, if any.
Method 2	The second method in the specified authentication login list, if any.
Method 3	The third method in the specified authentication login list, if any.

show authentication methods

Use this command to display information about the authentication methods.

Format `show authentication methods`

Mode Privileged EXEC

Example: The following example displays the authentication configuration.

```
(switch)#show authentication methods

Login Authentication Method Lists
---------------------------------
defaultList         :  local

Enable Authentication Method Lists
----------------------------------
enableList          :  local

Line     Login Method List    Enable Method List
-------  -----------------    ------------------
Console  defaultList          enableList
Telnet   defaultList          enableList
SSH      defaultList          enableList

HTTPS       :local
HTTP        :local
DOT1X       :none
```

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

Term	*Definition*
User	The user assigned to the specified authentication login list.
Component	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 the optional parameters *`unit/slot/port`* or *`vlanid`*, the command displays the global dot1x mode, the VLAN Assignment mode, and the Dynamic VLAN Creation mode.

Term	*Definition*
Administrative Mode	Indicates whether authentication control on the switch is enabled or disabled.
VLAN Assignment Mode	Indicates whether assignment of an authorized port to a RADIUS-assigned VLAN is allowed (enabled) or not (disabled).
Dynamic VLAN Creation Mode	Indicates whether the switch can dynamically create a RADIUS-assigned VLAN if it does not currently exist on the switch.
Monitor Mode	Indicates whether the Dot1x Monitor mode on the switch is enabled or disabled.

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

Term	*Definition*
Interface	The interface whose configuration is displayed.
Control Mode	The configured control mode for this port. Possible values are force-unauthorized | force-authorized | auto | mac-based | authorized | unauthorized.
Operating Control Mode	The control mode under which this port is operating. Possible values are authorized | unauthorized.

Term	*Definition*
Reauthentication Enabled	Indicates whether re-authentication is enabled on this port.
Port Status	Indicates whether the port is authorized or unauthorized. Possible values are authorized | unauthorized.

Example: The following shows example CLI display output for the command `show dot1x summary 0/1`.

```
                                   Operating
Interface      Control Mode      Control Mode      Port Status
---------      ------------      ------------      ------------
```

0/1 auto auto Authorized

If you use the optional parameter '`detail` slot/port', the detailed dot1x configuration for the specified port is displayed.

Term	*Definition*
Port	The interface whose configuration is displayed.
Protocol Version	The protocol version associated with this port. The only possible value is 1, corresponding to the first version of the dot1x specification.
PAE Capabilities	The port access entity (PAE) functionality of this port. Possible values are Authenticator or Supplicant.
Control Mode	The configured control mode for this port. Possible values are force-unauthorized | force-authorized | auto | mac-based.
Authenticator PAE State	Current state of the authenticator PAE state machine. Possible values are Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, ForceAuthorized, and ForceUnauthorized. When MAC-based authentication is enabled on the port, this parameter is deprecated.
Backend Authentication State	Current state of the backend authentication state machine. Possible values are Request, Response, Success, Fail, Timeout, Idle, and Initialize. When MAC-based authentication is enabled on the port, this parameter is deprecated.
Quiet Period	The timer used by the authenticator state machine on this port to define periods of time in which it will not attempt to acquire a supplicant. The value is expressed in seconds and will be in the range 0 and 65535.
Transmit Period	The timer used by the authenticator state machine on the specified port to determine when to send an EAPOL EAP Request/Identity frame to the supplicant. The value is expressed in seconds and will be in the range of 1 and 65535.
Guest-VLAN ID	The guest VLAN identifier configured on the interface.
Guest VLAN Period	The time in seconds for which the authenticator waits before authorizing and placing the port in the Guest VLAN, if no EAPOL packets are detected on that port.
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.

Term	*Definition*
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.
Vlan-assigned	The VLAN assigned to the port by the radius server. This is only valid when the port control mode is not Mac-based.
VLAN Assigned Reason	The reason the VLAN identified in the VLAN-assigned field has been assigned to the port. Possible values are RADIUS, Unauthenticated VLAN, Guest VLAN, default, and Not Assigned. When the VLAN Assigned Reason is Not Assigned, it means that the port has not been assigned to any VLAN by dot1x. This only valid when the port control mode is not MAC-based.
Reauthentication Period	The timer used by the authenticator state machine 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	The control direction for the specified port or ports. Possible values are both or in.
Maximum Users	The maximum number of clients that can get authenticated on the port in the MAC-based dot1x authentication mode. This value is used only when the port control mode is not MAC-based.
Unauthenticated VLAN ID	Indicates the unauthenticated VLAN configured for this port. This value is valid for the port only when the port control mode is not MAC-based.
Session Timeout	Indicates the time for which the given session is valid. The time period in seconds is returned by the RADIUS server on authentication of the port. This value is valid for the port only when the port control mode is not MAC-based.
Session Termination Action	This value indicates the action to be taken once the session timeout expires. Possible values are Default, Radius-Request. If the value is Default, the session is terminated the port goes into unauthorized state. If the value is Radius-Request, then a reauthentication of the client authenticated on the port is performed. This value is valid for the port only when the port control mode is not MAC-based.

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

```
(switch) #show dot1x detail 0/1
Port..................................... 0/1
Protocol Version......................... 1
PAE Capabilities......................... Supplicant
Control Mode............................. auto
Supplicant PAE State..................... Initialize
Supplicant Backend Authentication State........ Initialize
Maximum Start trails..................... 3
Start Period (secs)...................... 30
Held Period (secs)....................... 60
Authentication Period (secs)............. 30
EAP Method............................... MD5-Challenge
```

For each client authenticated on the port, the `show dot1x detail` slot/port command will display the following MAC-based dot1x parameters if the port-control mode for that specific port is MAC-based.

Term	*Definition*
Supplicant MAC-Address	The MAC-address of the supplicant.
Authenticator PAE State	Current state of the authenticator PAE state machine. Possible values are Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, ForceAuthorized, and ForceUnauthorized.
Backend Authentication State	Current state of the backend authentication state machine. Possible values are Request, Response, Success, Fail, Timeout, Idle, and Initialize.
VLAN-Assigned	The VLAN assigned to the client by the radius server.
Logical Port	The logical port number associated with the client.

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

Term	*Definition*
Port	The interface whose statistics are displayed.
EAPOL Frames Received	The number of valid EAPOL frames of any type that have been received by this authenticator.
EAPOL Frames Transmitted	The number of EAPOL frames of any type that have been transmitted by this authenticator.
EAPOL Start Frames Received	The number of EAPOL start frames that have been received by this authenticator.
EAPOL Logoff Frames Received	The number of EAPOL logoff frames that have been received by this authenticator.
Last EAPOL Frame Version	The protocol version number carried in the most recently received EAPOL frame.
Last EAPOL Frame Source	The source MAC address carried in the most recently received EAPOL frame.
EAP Response/Id Frames Received	The number of EAP response/identity frames that have been received by this authenticator.
EAP Response Frames Received	The number of valid EAP response frames (other than resp/id frames) that have been received by this authenticator.
EAP Request/Id Frames Transmitted	The number of EAP request/identity frames that have been transmitted by this authenticator.
EAP Request Frames Transmitted	The number of EAP request frames (other than request/identity frames) that have been transmitted by this authenticator.
Invalid EAPOL Frames Received	The number of EAPOL frames that have been received by this authenticator in which the frame type is not recognized.
EAP Length Error Frames Received	The number of EAPOL frames that have been received by this authenticator in which the frame type is not recognized.

show dot1x authentication-history

This command displays 802.1X authentication events and information during successful and unsuccessful Dot1x authentication process for all interfaces or the specified interface. Use the optional keywords to display only failure authentication events in summary or in detail.

Format `show dot1x authentication-history {slot/port | all} [failed-auth-only] [detail]`

Mode Privileged EXEC

Term	*Definition*
Time Stamp	The exact time at which the event occurs.
Interface	Physical Port on which the event occurs.
Mac-Address	The supplicant/client MAC address.
VLAN assigned	The VLAN assigned to the client/port on authentication.
VLAN assigned Reason	The type of VLAN ID assigned, which can be Guest VLAN, Unauth, Default, RADIUS Assigned, or Montior Mode VLAN ID.
Auth Status	The authentication status.
Reason	The actual reason behind the successful or failed authentication.

show dot1x clients

This command displays 802.1X client information. This command also displays information about the number of clients that are authenticated using Monitor mode and using 802.1X.

Format `show dot1x clients {slot/port | all} [detail]`

Mode Privileged EXEC

Term	*Definition*
Clients Authenticated using Monitor Mode	Indicates the number of the Dot1x clients authenticated using Monitor mode.
Clients Authenticated using Dot1x	Indicates the number of Dot1x clients authenticated using 802.1x authentication process.
Logical Interface	The logical port number associated with a client.
Interface	The physical port to which the supplicant is associated.
User Name	The user name used by the client to authenticate to the server.
Supplicant MAC Address	The supplicant device MAC address.
Session Time	The time since the supplicant is logged on.
Filter ID	Identifies the Filter ID returned by the RADIUS server when the client was authenticated. This is a configured DiffServ policy name on the switch.
VLAN ID	The VLAN assigned to the port.
VLAN Assigned	The reason the VLAN identified in the VLAN ID field has been assigned to the port. Possible values are RADIUS, Unauthenticated VLAN, Monitor Mode, or Default. When the VLAN Assigned reason is Default, it means that the VLAN was assigned to the port because the P-VID of the port was that VLAN ID.
Session Timeout	This value indicates the time for which the given session is valid. The time period in seconds is returned by the RADIUS server on authentication of the port. This value is valid for the port only when the port-control mode is not MAC-based.
Session Termination Action	This value indicates the action to be taken once the session timeout expires. Possible values are Default and Radius-Request. If the value is Default, the session is terminated and client details are cleared. If the value is Radius-Request, then a reauthentication of the client is performed.

show dot1x users

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

Format `show dot1x users slot/port`

Mode Privileged EXEC

Term	*Definition*
Users	Users configured locally to have access to the specified port.

802.1X Supplicant Commands

DWS-4000 supports 802.1X (dot1x) supplicant functionality on point-to-point ports. The administrator can configure the user name and password used in authentication and capabilities of the supplicant port.

dot1x pae

This command sets the port's dot1x role. The port can serve as either a supplicant or an authenticator.

Format `dot1x pae {supplicant | authenticator}`

Mode Interface Config

dot1x supplicant port-control

This command sets the ports authorization state (Authorized or Unauthorized) either manually or by setting the port to auto-authorize upon startup. By default all the ports are authenticators. If the port's attribute needs to be moved from <authenticator to supplicant> or <supplicant to authenticator>, use this command.

Format `dot1x supplicant port-control {auto | force-authorized | force_unauthorized}`

Mode Interface Config

Parameter	*Description*
auto	The port is in the Unauthorized state until it presents its user name and password credentials to an authenticator. If the authenticator authorizes the port, then it is placed in the Authorized state.
force-authorized	Sets the authorization state of the port to Authorized, bypassing the authentication process.
force-unauthorized	Sets the authorization state of the port to Unauthorized, bypassing the authentication process.

no dot1x supplicant port-control

This command sets the port-control mode to the default, auto.

Default auto

Format `no dot1x supplicant port-control`

Mode Interface Config

dot1x supplicant max-start

This command configures the number of attempts that the supplicant makes to find the authenticator before the supplicant assumes that there is no authenticator.

Default 3

Format `dot1x supplicant max-start {1—10}`

Mode Interface Config

no dot1x supplicant max-start

This command sets the max-start value to the default.

Format `no dot1x supplicant max-start`

Mode Interface Config

dot1x supplicant timeout start-period

This command configures the start period timer interval to wait for the EAP identity request from the authenticator.

Default 30 seconds

Format `dot1x supplicant timeout start-period` *`{1—65535 seconds}`*

Mode Interface Config

no dot1x supplicant timeout start-period

This command sets the start-period value to the default.

Format `no dot1x supplicant timeout start-period`

Mode Interface Config

dot1x supplicant timeout held-period

This command configures the held period timer interval to wait for the next authentication on previous authentication fail.

Default 30 seconds

Format `dot1x supplicant timeout held-period` *seconds*

Mode Interface Config

Parameter	*Description*
seconds	Number of seconds to wait for the next authenticaiton. Range: 1–65535 seconds.

no dot1x supplicant timeout held-period

This command sets the held-period value to the default value.

Format `no dot1x supplicant timeout held-period`

Mode Interface Config

dot1x supplicant timeout auth-period

This command configures the authentication period timer interval to wait for the next EAP request challenge from the authenticator.

Default 30 seconds

Format `dot1x supplicant timeout auth-period` *seconds*

Mode Interface Config

Parameter	*Description*
seconds	Number of seconds to wait for the next EAP request challenge. Range: 1–65535 seconds.

no dot1x supplicant timeout auth-period

This command sets the auth-period value to the default value.

Format `no dot1x supplicant timeout auth-period`

Mode Interface Config

dot1x supplicant user

Use this command to map the given user to the port.

Format `dot1x supplicant user`

Mode Interface Config

show dot1x statistics

This command displays the dot1x port statistics in detail.

Format `show dot1x statistics slot/port`

Mode
- Privileged EXEC
- User EXEC

Term	*Definition*
EAPOL Frames Received	Displays the number of valid EAPOL frames received on the port.
EAPOL Frames Transmitted	Displays the number of EAPOL frames transmitted via the port.
EAPOL Start Frames Transmitted	Displays the number of EAPOL Start frames transmitted via the port.
EAPOL Logoff Frames Received	Displays the number of EAPOL Log off frames that have been received on the port.
EAP Resp/ID Frames Received	Displays the number of EAP Respond ID frames that have been received on the port.
EAP Response Frames Received	Displays the number of valid EAP Respond frames received on the port.
EAP Req/ID Frames Transmitted	Displays the number of EAP Requested ID frames transmitted via the port.
EAP Req Frames Transmitted	Displays the number of EAP Request frames transmitted via the port.
Invalid EAPOL Frames Received	Displays the number of unrecognized EAPOL frames received on this port.
EAP Length Error Frames Received	Displays the number of EAPOL frames with an invalid Packet Body Length received on this port.
Last EAPOL Frames Version	Displays the protocol version number attached to the most recently received EAPOL frame.
Last EAPOL Frames Source	Displays the source MAC Address attached to the most recently received EAPOL frame.

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

```
(switch) #show dot1x statistics 0/1
Port..................................... 0/1
EAPOL Frames Received.................... 0
EAPOL Frames Transmitted................. 0
EAPOL Start Frames Transmitted........... 3
EAPOL Logoff Frames Received............. 0
EAP Resp/Id frames transmitted........... 0
EAP Response frames transmitted.......... 0
EAP Req/Id frames transmitted............ 0
```

```
EAP Req frames transmitted..................... 0
Invalid EAPOL frames received.................. 0
EAP length error frames received............... 0
Last EAPOL Frame Version....................... 0
Last EAPOL Frame Source....................... 00:00:00:00:02:01
```

Storm-Control Commands

This section describes commands you use to configure storm-control and view storm-control configuration information. A traffic storm is a condition that occurs when incoming packets flood the LAN, which creates performance degradation in the network. The Storm-Control feature protects against this condition.

DWS-4000 provides broadcast, multicast, and unicast story recovery for individual interfaces. Unicast Storm-Control protects against traffic whose MAC addresses are not known by the system. For broadcast, multicast, and unicast storm-control, if the rate of traffic ingressing on an interface increases beyond the configured threshold for that type, the traffic is dropped.

To configure storm-control, you will enable the feature for all interfaces or for individual interfaces, and you will set the threshold (storm-control level) beyond which the broadcast, multicast, or unicast traffic will be dropped. The Storm-Control feature allows you to limit the rate of specific types of packets through the switch on a per-port, per-type, basis.

Configuring a storm-control level also enables that form of storm-control. Disabling a storm-control level (using the `no` version of the command) sets the storm-control level back to the default value and disables that form of storm-control. Using the `no` version of the `storm-control` command (not stating a *`Level`*) disables that form of storm-control but maintains the configured *`Level`* (to be active the next time that form of storm-control is enabled.)

Note: The actual rate of ingress traffic required to activate storm-control is based on the size of incoming packets and the hard-coded average packet size of 512 bytes — used to calculate a packet-per-second (pps) rate - as the forwarding-plane requires pps versus an absolute rate kbps. For example, if the configured limit is 10%, this is converted to ~25000 pps, and this pps limit is set in forwarding plane (hardware). You get the approximate desired output when 512bytes packets are used.

storm-control broadcast

Use this command to enable broadcast storm recovery mode for a specific interface or range of 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`
Mode	Global Config Interface Config

no storm-control broadcast

Use this command to disable broadcast storm recovery mode for a specific interface or range of interfaces.

Format `no storm-control broadcast`

Mode Global Config
Interface Config

storm-control broadcast level

Use this command to configure the broadcast storm recovery threshold for an interface as a percentage of link speed and enable broadcast storm recovery. If the mode is enabled, broadcast storm recovery is active, and if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic is dropped. Therefore, the rate of broadcast traffic is limited to the configured threshold.

Default 5

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 rate

Use this command to configure the broadcast storm recovery threshold for an interface in packets per second. If the mode is enabled, broadcast storm recovery is active, and if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic is dropped. Therefore, the rate of broadcast traffic is limited to the configured threshold.

Default 0

Format `storm-control broadcast rate` *`0—33554431`*

Mode Interface Config

no storm-control broadcast rate

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

Format `no storm-control broadcast rate`

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 as a percentage of link speed and enables broadcast storm recovery. If the mode is enabled, broadcast storm recovery is active, and if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic 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 broadcast all rate

Use this command to configure the broadcast storm recovery threshold for all interfaces in packets per second. If the mode is enabled, broadcast storm recovery is active, and if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic is dropped. Therefore, the rate of broadcast traffic is limited to the configured threshold.

Default 0

Format `storm-control broadcast rate` *`0—33554431`*

Mode Global Config

no storm-control broadcast all rate

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 rate`

Mode Global Config

storm-control multicast

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

Default disabled

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 as a percentage of link speed and enables multicast storm recovery mode. If the mode is enabled, multicast storm recovery is active, and if the rate of L2 multicast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of multicast traffic will be limited to the configured threshold.

Default 5

Format `storm-control multicast level 0–100`

Mode 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 0–100`

Mode Interface Config

storm-control multicast rate

Use this command to configure the multicast storm recovery threshold for an interface in packets per second. If the mode is enabled, multicast storm recovery is active, and if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic is dropped. Therefore, the rate of multicast traffic is limited to the configured threshold.

Default 0

Format `storm-control multicast rate 0–33554431`

Mode Interface Config

no storm-control multicast rate

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

Format `no storm-control multicast rate`

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 as a percentage of link speed and enables multicast storm recovery mode. If the mode is enabled, multicast storm recovery is active, and if the rate of L2 multicast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of multicast traffic will be limited to the configured threshold.

Default 5

Format `storm-control multicast 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 multicast all rate

Use this command to configure the multicast storm recovery threshold for all interfaces in packets per second. If the mode is enabled, multicast storm recovery is active, and if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic is dropped. Therefore, the rate of multicast traffic is limited to the configured threshold.

Default 0

Format `storm-control multicast rate` *`0—33554431`*

Mode Global Config

no storm-control broadcast all rate

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 rate`

Mode Global Config

storm-control unicast

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

Default disabled

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

Default 5

Format `storm-control unicast level` *`0—100`*

Mode 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 rate

Use this command to configure the unicast storm recovery threshold for an interface in packets per second. If the mode is enabled, unicast storm recovery is active, and if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic is dropped. Therefore, the rate of unicast traffic is limited to the configured threshold.

Default 0

Format `storm-control unicast rate` *`0—33554431`*

Mode Interface Config

no storm-control unicast rate

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

Format `no storm-control unicast rate`

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

Default 5

Format `storm-control unicast all level` *`0—100`*

Mode Global Config

no storm-control unicast all level

This command sets 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 unicast all rate

Use this command to configure the unicast storm recovery threshold for all interfaces in packets per second. If the mode is enabled, unicast storm recovery is active, and if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic is dropped. Therefore, the rate of unicast traffic is limited to the configured threshold.

Default 0

Format `storm-control unicast all rate` *`0—33554431`*

Mode Global Config

no storm-control unicast all rate

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

Format `no storm-control unicast all rate`

Mode Global Config

storm-control flowcontrol

This command enables 802.3x flow control for the switch and applies only 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 applies only 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:

- **Broadcast Storm Recovery Mode** may be enabled or disabled. The factory default is disabled.
- **802.3x Flow Control Mode** may be enabled or disabled. The factory default is disabled.

Use the `all` keyword to display the per-port configuration parameters for all interfaces, or specify the slot/port to display information about a specific interface.

Format `show storm-control [all | slot/port]`

Mode Privileged EXEC

Term	*Definition*
Bcast Mode	Shows whether the broadcast storm control mode is enabled or disabled. The factory default is disabled.
Bcast Level	The broadcast storm control level.
Mcast Mode	Shows whether the multicast storm control mode is enabled or disabled.
Mcast Level	The multicast storm control level.
Ucast Mode	Shows whether the Unknown Unicast or DLF (Destination Lookup Failure) storm control mode is enabled or disabled.
Ucast Level	The Unknown Unicast or DLF (Destination Lookup Failure) storm control level.

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

```
(Routing) #show storm-control
802.3x Flow Control Mode..................... Disable
```

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

```
(Routing) #show storm-control 1/0/1

        Bcast   Bcast    Mcast   Mcast    Ucast   Ucast
 Intf   Mode    Level    Mode    Level    Mode    Level
------ ------- -------- ------- -------- ------- --------
1/0/1  Disable       5% Disable       5% Disable       5%
```

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

```
(Routing) #show storm-control all

        Bcast   Bcast    Mcast   Mcast    Ucast   Ucast
 Intf   Mode    Level    Mode    Level    Mode    Level
------ ------- -------- ------- -------- ------- --------
1/0/1  Disable       5% Disable       5% Disable       5%
1/0/2  Disable       5% Disable       5% Disable       5%
1/0/3  Disable       5% Disable       5% Disable       5%
1/0/4  Disable       5% Disable       5% Disable       5%
1/0/5  Disable       5% Disable       5% Disable       5%
```

Link Local Protocol Filtering Commands

Link Local Protocol Filtering (LLPF) allows the switch to filter out multiple proprietary protocol PDUs, such as Port Aggregation Protocol (PAgP), if the problems occur with proprietary protocols running on standards-based switches. If certain protocol PDUs cause unexpected results, LLPF can be enabled to prevent those protocol PDUs from being processed by the switch.

llpf blockall

Use this command to block LLPF protocol(s) on a port.

Default disable

Format `llpf {blockisdp | blockvtp | blockdtp | blockudld | blockpagp | blocksstp | blockall}`

Mode Interface Config

no llpf blockall

Use this command to unblock LLPF protocol(s) on a port.

Format `no llpf {blockisdp | blockvtp | blockdtp | blockudld | blockpagp | blocksstp | blockall }`

Mode Interface Config

show llpf interface all

Use this command to display the status of LLPF rules configured on a particular port or on all ports.

Format `show llpf interface [all | slot/port]`

Mode Privileged EXEC

Term	*Definition*
Block ISDP	Shows whether the port blocks ISDP PDUs.
Block VTP	Shows whether the port blocks VTP PDUs.
Block DTP	Shows whether the port blocks DTP PDUs.
Block UDLD	Shows whether the port blocks UDLD PDUs.
Block PAGP	Shows whether the port blocks PAgP PDUs.
Block SSTP	Shows whether the port blocks SSTP PDUs.
Block All	Shows whether the port blocks all proprietary PDUs available for the LLDP feature.

Port-Channel/LAG (802.3ad) Commands

This section describes the commands you use to configure port-channels, which is defined in the 802.3ad specification, and that are also known as link aggregation groups (LAGs). Link aggregation allows you to combine multiple full-duplex Ethernet links into a single logical link. Network devices treat the aggregation as if it were a single link, which increases fault tolerance and provides load sharing. The LAG feature initially load shares traffic based upon the source and destination MAC address. Assign the port-channel (LAG) VLAN membership after you create a port-channel. If you do not assign VLAN membership, the port-channel might become a member of the management VLAN which can result in learning and switching issues.

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

Note: If you configure the maximum number of 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 216.

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/port number of a configured port-channel. You can add a range of ports by specifying the port range when you enter Interface Config mode (for example: `interface 1/0/1-1/0/4`.

Note: Before adding a port to a port-channel, set the physical mode of the port. For more information, see "speed" on page 216.

Format `addport logical slot/port`

Mode Interface Config

deleteport (Interface Config)

This command deletes a port or a range of ports from the port-channel (LAG). The interface is a logical slot/port number of a configured port-channel (or range of port-channels).

Format `deleteport logical slot/port`

Mode Interface Config

deleteport (Global Config)

This command deletes all configured ports from the port-channel (LAG). The interface is a logical slot/port number of a configured port-channel. To clear the port channels, see "clear port-channel" on page 149.

Format `deleteport {logical slot/port | all}`

Mode Global Config

lacp admin key

Use this command to configure the administrative value of the key for the port-channel. The value range of *key* is 0 to 65535. This command can be used to configure a single interface or a range of interfaces.

Default 0x8000

Format `lacp admin key key`

Mode Interface Config

Note: This command is applicable only to port-channel interfaces.

no lacp admin key

Use this command to configure the default administrative value of the key for the port-channel.

Format `no lacp admin key`

Mode Interface Config

lacp collector max-delay

Use this command to configure the port-channel collector max delay. This command can be used to configure a single interface or a range of interfaces.The valid range of *delay* is 0–65535.

Default 0x8000

Format `lacp collector max delay delay`

Mode Interface Config

Note: This command is applicable only to port-channel interfaces.

no lacp collector max delay

Use this command to configure the default port-channel collector max delay.

Format `no lacp collector max delay`

Mode Interface Config

lacp actor admin

Use this command to configure the LACP actor admin parameters.

lacp actor admin key

Use this command to configure the administrative value of the LACP actor admin key on an interface or range of interfaces. The valid range for *key* is 0–65535.

Default Internal Interface Number of this Physical Port

Format `lacp actor admin key key`

Mode Interface Config

Note: This command is applicable only to physical interfaces.

no lacp actor admin key

Use this command to configure the default administrative value of the key.

Format `no lacp actor admin key`

Mode Interface Config

lacp actor admin state

Use this command to configure the administrative value of actor state as transmitted by the Actor in LACPDUs. The valid value range is 0x00–0xFF. This command can be used to configure a single interfaces or a range of interfaces.

Default 0x07

Format `lacp actor admin state {individual|longtimeout|passive}`

Mode Interface Config

Note: This command is applicable only to physical interfaces.

no lacp actor admin state

Use this command the configure the default administrative values of actor state as transmitted by the Actor in LACPDUs.

Format `no lacp actor admin state {individual|longtimeout|passive}`

Mode Interface Config

lacp actor admin state individual

Use this command to set LACP actor admin state to individual.

Format `lacp actor admin state individual`

Mode Interface Config

Note: This command is applicable only to physical interfaces.

no lacp actor admin state individual

Use this command to set the LACP actor admin state to aggregation.

Format `no lacp actor admin state individual`

Mode Interface Config

lacp actor admin state longtimeout

Use this command to set LACP actor admin state to longtimeout.

Format `lacp actor admin state longtimeout`

Mode Interface Config

Note: This command is applicable only to physical interfaces.

no lacp actor admin state longtimeout

Use this command to set the LACP actor admin state to short timeout.

Format `no lacp actor admin state longtimeout`

Mode Interface Config

Note: This command is applicable only to physical interfaces.

lacp actor admin state passive

Use this command to set the LACP actor admin state to passive.

Format `lacp actor admin state passive`

Mode Interface Config

Note: This command is applicable only to physical interfaces.

no lacp actor admin state passive

Use this command to set the LACP actor admin state to active.

Format `no lacp actor admin state passive`

Mode Interface Config

lacp actor port

Use this command to configure LACP actor port priority key.

Format `lacp actor port`

Mode Interface Config

lacp actor port priority

Use this command to configure the priority value assigned to the Aggregation Port for an interface or range of interfaces. The valid range for *priority* is 0 to 255.

Default 0x80

Format `lacp actor port priority` *0—255*

Mode Interface Config

Note: This command is applicable only to physical interfaces.

no lacp actor port priority

Use this command to configure the default priority value assigned to the Aggregation Port.

Format `no lacp actor port priority`

Mode Interface Config

lacp partner admin key

Use this command to configure the administrative value of the Key for the protocol partner. This command can be used to configure a single interface or a range of interfaces. The valid range for *key* is 0 to 65535.

Default 0x0

Format `lacp partner admin key` *key*

Mode Interface Config

Note: This command is applicable only to physical interfaces.

no lacp partner admin key

Use this command to configure the administrative value of the Key for the protocol partner.

Format `no lacp partner admin key` *key*

Mode Interface Config

lacp partner admin state

Use this command to configure the current administrative value of actor state for the protocol Partner. The valid value range is 0x00–0xFF.

Default 0x07

Format `lacp partner admin state {individual|longtimeout|passive}`

Mode Interface Config

Note: This command is applicable only to physical interfaces.

no lacp partner admin state

Use this command the configure the default current administrative value of actor state for the protocol partner. This command can be used to configure a single interface or a range of interfaces.

Format `no lacp partner admin state {individual|longtimeout|passive}`

Mode Interface Config

lacp partner admin state individual

Use this command to set LACP partner admin state to individual.

Format `lacp partner admin state individual`

Mode Interface Config

Note: This command is applicable only to physical interfaces.

no lacp partner admin state individual

Use this command to set the LACP partner admin state to aggregation.

Format `no lacp partner admin state individual`

Mode Interface Config

lacp partner admin state longtimeout

Use this command to set LACP partner admin state to longtimeout.

Format `lacp partner admin state longtimeout`

Mode Interface Config

Note: This command is applicable only to physical interfaces.

no lacp partner admin state longtimeout

Use this command to set the LACP partner admin state to short timeout.

Format `no lacp partner admin state longtimeout`

Mode Interface Config

Note: This command is applicable only to physical interfaces.

lacp partner admin state passive

Use this command to set the LACP partner admin state to passive.

Format `lacp partner admin state passive`

Mode Interface Config

Note: This command is applicable only to physical interfaces.

no lacp partner admin state passive

Use this command to set the LACP partner admin state to active.

Format `no lacp partner admin state passive`

Mode Interface Config

lacp partner port id

Use this command to configure the LACP partner port id. This command can be used to configure a single interface or a range of interfaces. The valid range for *port-id* is 0 to 65535.

Default 0x80

Format `lacp partner port-id` *port-id*

Mode Interface Config

Note: This command is applicable only to physical interfaces.

no lacp partner port id

Use this command to set the LACP partner port id to the default.

Format `lacp partner port-id`

Mode Interface Config

lacp partner port priority

Use this command to configure the LACP partner port priority. This command can be used to configure a single interface or a range of interfaces. The valid range for *priority* is 0 to 255.

Default 0x0

Format `lacp partner port priority` *priority*

Mode Interface Config

Note: This command is applicable only to physical interfaces.

no lacp partner port priority

Use this command to configure the default LACP partner port priority.

Format `no lacp partner port priority`

Mode Interface Config

lacp partner system-id

Use this command to configure the 6-octet MAC Address value representing the administrative value of the Aggregation Port's protocol Partner's System ID. This command can be used to configure a single interface or a range of interfaces. The valid range of *system-id* is 00:00:00:00:00:00 - FF:FF:FF:FF:FF:FF.

Default 00:00:00:00:00:00

Format `lacp partner system-id system-id`

Mode Interface Config

Note: This command is applicable only to physical interfaces.

no lacp partner system-id

Use this command to configure the default value representing the administrative value of the Aggregation Port's protocol Partner's System ID.

Format `no lacp partner system-id`

Mode Interface Config

lacp partner system priority

Use this command to configure the administrative value of the priority associated with the Partner's System ID. This command can be used to configure a single interface or a range of interfaces. The valid range for *priority* is 0 to 65535.

Default 0x0

Format `lacp partner system priority 0–65535`

Mode Interface Config

Note: This command is applicable only to physical interfaces.

no lacp partner system priority

Use this command to configure the default administrative value of priority associated with the Partner's System ID.

Format `no lacp partner system priority`

Mode Interface Config

port-channel static

This command enables the static mode on a port-channel (LAG) interface or range of interfaces. By default the static mode for a new port-channel is 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 or range of ports.

Default enabled

Format `port lacpmode`

Mode Interface Config

no port lacpmode

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

Format `no port lacpmode`

Mode Interface Config

port lacpmode 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 lacptimeout (Interface Config)

This command sets the timeout on a physical interface or range of interfaces of a particular device type (actor or partner) to either long or short timeout.

Default long

Format `port lacptimeout {actor | partner} {long | short}`

Mode Interface Config

no port lacptimeout

This command sets the timeout back to its default value on a physical interface of a particular device type (actor or partner).

Format `no port lacptimeout {actor | partner}`

Mode Interface Config

port lacptimeout (Global Config)

This command sets the timeout for all interfaces of a particular device type (actor or partner) to either long or short timeout.

Default long

Format `port lacptimeout {actor | partner} {long | short}`

Mode Global Config

no port lacptimeout

This command sets the timeout for all physical interfaces of a particular device type (actor or partner) back to their default values.

Format `no port lacptimeout {actor | partner}`

Mode Global Config

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 load-balance

This command selects the load-balancing option used on a port-channel (LAG). Traffic is balanced on a port-channel (LAG) by selecting one of the links in the channel over which to transmit specific packets. The link is selected by creating a binary pattern from selected fields in a packet, and associating that pattern with a particular link.

Load-balancing is not supported on every device. The range of options for load-balancing may vary per device.

This command can be configured for a single interface, a range of interfaces, or all interfaces.

Default 3

Format `port-channel load-balance {1 | 2 | 3 | 4 | 5 | 6 | 7} {slot/port | all}`

Mode Interface Config
Global Config

Term	*Definition*
1	Source MAC, VLAN, EtherType, and incoming port associated with the packet
2	Destination MAC, VLAN, EtherType, and incoming port associated with the packet
3	Source/Destination MAC, VLAN, EtherType, and incoming port associated with the packet
4	Source IP and Source TCP/UDP fields of the packet
5	Destination IP and Destination TCP/UDP Port fields of the packet
6	Source/Destination IP and source/destination TCP/UDP Port fields of the packet
7	Enhanced hashing mode
slot/port| all	Global Config Mode only: The interface is a logical slot/port number of a configured port-channel. `All` applies the command to all currently configured port-channels.

no port-channel load-balance

This command reverts to the default load balancing configuration.

Format `no port-channel load-balance {slot/port | all}`

Mode Interface Config
Global Config

Term	*Definition*
slot/port| all	Global Config Mode only: The interface is a logical slot/port number of a configured port-channel. **All** applies the command to all currently configured port-channels.

port-channel 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

port-channel system priority

Use this command to configure port-channel system priority. The valid range of *priority* is 0–65535.

Default 0x8000

Format `port-channel system priority priority`

Mode Global Config

no port-channel system priority

Use this command to configure the default port-channel system priority value.

Format `no port-channel system priority`

Mode Global Config

show lacp actor

Use this command to display LACP actor attributes.

Format `show lacp actor {slot/port|all}`

Mode Global Config

The following output parameters are displayed.

Parameter	*Description*
System Priority	The administrative value of the Key.
Actor Admin Key	The administrative value of the Key.
Port Priority	The priority value assigned to the Aggregation Port.
Admin State	The administrative values of the actor state as transmitted by the Actor in LACPDUs.

show lacp partner

Use this command to display LACP partner attributes.

Format `show lacp actor {slot/port|all}`

Mode Privileged EXEC

The following output parameters are displayed.

Parameter	*Description*
System Priority	The administrative value of priority associated with the Partner's System ID.
System-ID	Represents the administrative value of the Aggregation Port's protocol Partner's System ID.
Admin Key	The administrative value of the Key for the protocol Partner.
Port Priority	The administrative value of the Key for protocol Partner.
Port-ID	The administrative value of the port number for the protocol Partner.
Admin State	The administrative values of the actor state for the protocol Partner.

show port-channel brief

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

Format `show port-channel brief`

Mode
- Privileged EXEC
- User EXEC

For each port-channel the following information is displayed:

Term	*Definition*
Logical Interface	The slot/port of the logical interface.
Port-channel Name	The name of port-channel (LAG) interface.

Term	*Definition*
Link-State	Shows whether the link is up or down.
Trap Flag	Shows whether trap flags are enabled or disabled.
Type	Shows whether the port-channel is statically or dynamically maintained.
Mbr Ports	The members of this port-channel.
Active Ports	The ports that are actively participating in the port-channel.

show port-channel

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

Format `show port-channel {`*`Logical`* `slot/port | all}`

Mode
- Privileged EXEC
- User EXEC

Term	*Definition*
Logical Interface	The valid slot/port number.
Port-Channel Name	The name of this port-channel (LAG). You may enter any string of up to 15 alphanumeric characters.
Link State	Indicates whether the Link is up or down.
Admin Mode	May be enabled or disabled. The factory default is enabled.
Type	The status designating whether a particular port-channel (LAG) is statically or dynamically maintained. • **Static** - The port-channel is statically maintained. • **Dynamic** - The port-channel is dynamically maintained.
Mbr Ports	A listing of the ports that are members of this port-channel (LAG), in slot/port notation. There can be a maximum of eight ports assigned to a given port-channel (LAG).
Device Timeout	For each port, lists the timeout (**long** or **short**) for Device Type (**actor** or **partner**).
Port Speed	Speed of the port-channel port.
Active Ports	This field lists ports that are actively participating in the port-channel (LAG).
Load Balance Option	The load balance option associated with this LAG. See “port-channel load-balance” on page 308.

show port-channel system priority

Use this command to display the port-channel system priority.

Format `show port-channel system priority`

Mode Privileged EXEC

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` 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 DWS-4000 software only supports one session, if you do not supply optional parameters, the behavior of this command is similar to the behavior of the `no monitor` command.

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

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

Term	*Definition*
Session ID	An integer value used to identify the session. Its value can be anything between 1 and the maximum number of mirroring sessions allowed on the platform.
Monitor Session Mode	Indicates whether the Port Mirroring feature is enabled or disabled for the session identified with *`session-id`*. The possible values are Enabled and Disabled.
Probe Port	Probe port (destination port) for the session identified with *`session-id`*. If probe port is not set then this field is blank.
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. Static MAC filtering allows you to configure destination ports for a static multicast MAC filter irrespective of the platform.

macfilter

This command adds a static MAC filter entry for the MAC address *macaddr* on the VLAN *vlanid*. The value of the *macaddr* parameter is a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6. The restricted MAC Addresses are: 00:00:00:00:00:00, 01:80:C2:00:00:00 to 01:80:C2:00:00:0F, 01:80:C2:00:00:20 to 01:80:C2:00:00:21, and FF:FF:FF:FF:FF:FF. The *vlanid* parameter must identify a valid VLAN.

The number of static mac filters supported on the system is different for MAC filters where source ports are configured and MAC filters where destination ports are configured.

- For unicast MAC address filters and multicast MAC address filters with source port lists, the maximum number of static MAC filters supported is 20.
- For multicast MAC address filters with destination ports configured, the maximum number of static filters supported is 256.

i.e. For current Broadcom platforms, you can configure the following combinations:

- Unicast MAC and source port (max = 20)
- Multicast MAC and source port (max = 20)
- Multicast MAC and destination port (only) (max = 256)
- Multicast MAC and source ports and destination ports (max = 20)

Format `macfilter macaddr vlanid`

Mode Global Config

no macfilter

This command removes all filtering restrictions and the static MAC filter entry for the MAC address *macaddr* on the VLAN *vlanid*. The *macaddr* parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6.

The *vlanid* parameter must identify a valid VLAN.

Format `no macfilter macaddr vlanid`

Mode Global Config

macfilter adddest

Use this command to add the interface or range of interfaces to the destination filter set for the MAC filter with the given *macaddr* and VLAN of *vlanid*. The *macaddr* parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6. The *vlanid* parameter must identify a valid VLAN.

Note: Configuring a destination port list is only valid for multicast MAC addresses.

Format `macfilter adddest macaddr`

Mode Interface Config

no macfilter adddest

This command removes a port from the destination filter set for the MAC filter with the given *macaddr* and VLAN of *vlanid*. The *macaddr* parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6. The *vlanid* parameter must identify a valid VLAN.

Format `no macfilter adddest macaddr`

Mode Interface Config

macfilter adddest all

This command adds all interfaces to the destination filter set for the MAC filter with the given *macaddr* and VLAN of *vlanid*. The *macaddr* parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6. The *vlanid* parameter must identify a valid VLAN.

Note: Configuring a destination port list is only valid for multicast MAC addresses.

Format `macfilter adddest all macaddr`

Mode Global Config

no macfilter adddest all

This command removes all ports from the destination filter set for the MAC filter with the given *macaddr* and VLAN of *vlanid*. The *macaddr* parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6. The *vlanid* parameter must identify a valid VLAN.

Format `no macfilter adddest all macaddr`

Mode Global Config

macfilter addsrc

This command adds the interface or range of interfaces to the source filter set for the MAC filter with the MAC address of *macaddr* and VLAN of *vlanid*. The *macaddr* parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6. The *vlanid* parameter must identify a valid VLAN.

Format `macfilter addsrc macaddr vlanid`

Mode Interface Config

no macfilter addsrc

This command removes a port from the source filter set for the MAC filter with the MAC address of *macaddr* and VLAN of *vlanid*. The *macaddr* parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6. The *vlanid* parameter must identify a valid VLAN.

Format `no macfilter addsrc macaddr vlanid`

Mode Interface Config

macfilter addsrc all

This command adds all interfaces to the source filter set for the MAC filter with the MAC address of *macaddr* and *vlanid*. You must specify the *macaddr* parameter as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6. The *vlanid* parameter must identify a valid VLAN.

Format `macfilter addsrc all macaddr vlanid`

Mode Global Config

no macfilter addsrc all

This command removes all interfaces to the source filter set for the MAC filter with the MAC address of *macaddr* and VLAN of *vlanid*. You must specify the *macaddr* parameter as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6.

The *vlanid* parameter must identify a valid VLAN.

Format `no macfilter addsrc all macaddr vlanid`

Mode Global Config

show mac-address-table static

This command displays the Static MAC Filtering information for all Static MAC Filters. If you specify `all`, all the Static MAC Filters in the system are displayed. If you supply a value for *`macaddr`*, you must also enter a value for *`vlanid`*, and the system displays Static MAC Filter information only for that MAC address and VLAN.

Format `show mac-address-table static {`*`macaddr vlanid`* `| all}`

Mode Privileged EXEC

Term	*Definition*
MAC Address	The MAC Address of the static MAC filter entry.
VLAN ID	The VLAN ID of the static MAC filter entry.
Source Port(s)	The source port filter set's slot and port(s).

Note: Only multicast address filters will have destination port lists.

show mac-address-table staticfiltering

This command displays the Static Filtering entries in the Multicast Forwarding Database (MFDB) table.

Format `show mac-address-table staticfiltering`

Mode Privileged EXEC

Term	*Definition*
VLAN ID	The VLAN in which the MAC Address is learned.
MAC Address	A unicast MAC address for which the switch has forwarding and or filtering information. As the data is gleaned from the MFDB, the address will be a multicast address. The format is 6 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB.
Type	The type of the entry. Static entries are those that are configured by the end user. Dynamic entries are added to the table as a result of a learning process or protocol.
Description	The text description of this multicast table entry.
Interfaces	The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).

DHCP L2 Relay Agent Commands

You can enable the switch to operate as a DHCP Layer 2 relay agent to relay DHCP requests from clients to a Layer 3 relay agent or server. The Circuit ID and Remote ID can be added to DHCP requests relayed from clients to a DHCP server. This information is included in DHCP Option 82, as specified in sections 3.1 and 3.2 of RFC3046.

dhcp l2relay

This command enables the DHCP Layer 2 Relay agent for an interface a range of interfaces in, or all interfaces. The subsequent commands mentioned in this section can only be used when the DHCP L2 relay is enabled.

Format `dhcp l2relay`

Mode
- Global Config
- Interface Config

no dhcp l2relay

This command disables DHCP Layer 2 relay agent for an interface or range of interfaces.

Format `no dhcp l2relay`

Mode
- Global Config
- Interface Config

dhcp l2relay circuit-id subscription-name

This command sets the Option-82 Circuit ID for a given service subscription identified by *`subscription-string`* on a given interface. The *`subscription-string`* is a character string which needs to be matched with a configured DOT1AD subscription string for correct operation. When circuit-id is enabled using this command, all Client DHCP requests that fall under this service subscription are added with Option-82 circuit-id as the incoming interface number.

Default disabled

Format `dhcp l2relay circuit-id subscription-name subscription-string`

Mode Interface Config

no dhcp l2relay circuit-id subscription-name

This command resets the Option-82 Circuit ID for a given service subscription identified by *`subscription-string`* on a given interface. The *`subscription-string`* is a character string which needs to be matched with a configured DOT1AD subscription string for correct operation. When circuit-id is disabled using this command, all Client DHCP requests that fall under this service subscription are no longer added with Option-82 circuit-id.

Format `no dhcp l2relay circuit-id subscription-name subscription-string`

Mode Interface Config

dhcp l2relay circuit-id vlan

This parameter sets the DHCP Option-82 Circuit ID for a VLAN. When enabled, the interface number is added as the Circuit ID in DHCP option 82.

Format `dhcp l2relay circuit-id vlan vlan-list`

Mode Global Config

Parameter	*Description*
vlan–list	The VLAN ID. The range is 1–4093. Separate non-consecutive IDs with a comma (,) no spaces and no zeros in between the range. Use a dash (–) for the range.

no dhcp l2relay circuit-id vlan

This parameter clears the DHCP Option-82 Circuit ID for a VLAN.

Format `no dhcp l2relay circuit-id vlan vlan-list`

Mode Global Config

dhcp l2relay remote-id subscription-name

This command sets the Option-82 Remote-ID string for a given service subscription identified by *subscription-string* on a given interface or range of interfaces. The *subscription-string* is a character string which needs to be matched with a configured DOT1AD subscription string for correct operation. The *remoteid-string* is a character string. When *remote-id string* is set using this command, all Client DHCP requests that fall under this service subscription are added with Option-82 Remote-id as the configured remote-id string.

Default empty string

Format `dhcp l2relay remote-id remoteid-string subscription-name subscription-string`

Mode Interface Config

no dhcp l2relay remote-id subscription-name

This command resets the Option-82 Remote-ID string for a given service subscription identified by *subscription-string* on a given interface. The *subscription-string* is a character string which needs to be matched with a configured DOT1AD subscription string for correct operation. When *remote-id* string is reset using this command, the Client DHCP requests that fall under this service subscription are not added with Option-82 Remote-id.

Format `no dhcp l2relay remote-id remoteid-string subscription-name subscription-string`

Mode Interface Config

dhcp l2relay remote-id vlan

This parameter sets the DHCP Option-82 Remote ID for a VLAN and subscribed service (based on subscription-name).

Format `dhcp l2relay remote-id remote-id-string vlan vlan-list`

Mode Global Config

Parameter	*Description*
vlan–list	The VLAN ID. The range is 1–4093. Separate non-consecutive IDs with a comma (,) no spaces and no zeros in between the range. Use a dash (–) for the range.

no dhcp l2relay remote-id vlan

This parameter clears the DHCP Option-82 Remote ID for a VLAN and subscribed service (based on subscription-name).

Format `no dhcp l2relay remote-id vlan vlan-list`

Mode Global Config

Format `no dhcp l2relay subscription-name subscription-string`

Mode Interface Config

dhcp l2relay trust

Use this command to configure an interface or range of interfaces as trusted for Option-82 reception.

Default untrusted

Format `dhcp l2relay trust`

Mode Interface Config

no dhcp l2relay trust

Use this command to configure an interface to the default untrusted for Option-82 reception.

Format `no dhcp l2relay trust`

Mode Interface Config

dhcp l2relay vlan

Use this command to enable the DHCP L2 Relay agent for a set of VLANs. All DHCP packets which arrive on interfaces in the configured VLAN are subject to L2 Relay processing.

Default `disable`

Format `dhcp l2relay vlan vlan-list`

Mode Global Config

Parameter	*Description*
vlan–list	The VLAN ID. The range is 1–4093. Separate non-consecutive IDs with a comma (,) no spaces and no zeros in between the range. Use a dash (–) for the range.

no dhcp l2relay vlan

Use this command to disable the DHCP L2 Relay agent for a set of VLANs.

Format `no dhcp l2relay vlan` *`vlan-list`*

Mode Global Config

show dhcp l2relay all

This command displays the summary of DHCP L2 Relay configuration.

Format `show dhcp l2relay all`

Mode Privileged EXEC

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

```
(Switching) #show dhcp l2relay all

DHCP L2 Relay is Enabled.

Interface  L2RelayMode   TrustMode
---------  -----------  --------------
 0/2        Enabled      untrusted
 0/4        Disabled     trusted

VLAN Id    L2 Relay  CircuitId  RemoteId
--------- ----------  ----------- ------------
 3           Disabled    Enabled    --NULL--
 5           Enabled     Enabled    --NULL--
 6           Enabled     Enabled    broadcom
 7           Enabled     Disabled   --NULL--
 8           Enabled     Disabled   --NULL--
 9           Enabled     Disabled   --NULL--
 10          Enabled     Disabled   --NULL--
```

show dhcp l2relay interface

This command displays DHCP L2 relay configuration specific to interfaces.

Format `show dhcp l2relay interface {all | interface-num}`

Mode Privileged EXEC

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

```
(Switching) #show dhcp l2relay interface all

DHCP L2 Relay is  Enabled.

Interface  L2RelayMode   TrustMode
---------  -----------  --------------
 0/2        Enabled      untrusted
 0/4        Disabled     trusted
```

show dhcp l2relay stats interface

This command displays statistics specific to DHCP L2 Relay configured interface.

Format `show dhcp l2relay stats interface {all | interface-num}`

Mode Privileged EXEC

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

```
(Switching) #show dhcp l2relay stats interface all

DHCP L2 Relay is  Enabled.

Interface  UntrustedServer    UntrustedClient  TrustedServer     TrustedClient
            MsgsWithOpt82    MsgsWithOpt82    MsgsWithoutOpt82  MsgsWithoutOpt82
---------  --------------- -----------------  ----------------- --------------
 0/1           0                 0                 0                0
 0/2           0                 0                 3                7
 0/3           0                 0                 0                0
 0/4           0                 12                0                0
 0/5           0                 0                 0                0
 0/6           3                 0                 0                      0
 0/7           0                 0                 0                0
 0/8           0                 0                 0                0
 0/9           0                 0                 0                0
```

show dhcp l2relay agent-option vlan

This command displays the DHCP L2 Relay Option-82 configuration specific to VLAN.

Format `show dhcp l2relay agent-option vlan vlan-range`

Mode Privileged EXEC

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

```
(Switching) #show dhcp l2relay agent-option vlan 5-10

DHCP L2 Relay is  Enabled.

VLAN Id    L2 Relay       CircuitId  RemoteId
--------- ----------  ----------- ------------
5           Enabled     Enabled    --NULL--
6           Enabled     Enabled    broadcom
7           Enabled     Disabled   --NULL--
8           Enabled     Disabled   --NULL--
9           Enabled     Disabled   --NULL--
10          Enabled     Disabled   --NULL--
```

show dhcp l2relay vlan

This command shows whether DHCP L2 Relay is globally enabled and enabled on the specified VLAN or VLAN range.

Format `show dhcp l2relay vlan` *`vlan-range`*

Mode Privileged EXEC

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

```
(Routing) #show dhcp l2relay vlan 100

DHCP L2 Relay is  Enabled.

DHCP L2 Relay is enabled on the following VLANs:
100
```

show dhcp l2relay circuit-id vlan

This command shows whether DHCP L2 Relay is globally enabled and whether the DHCP Circuit-Id option is enabled on the specified VLAN or VLAN range.

Format `show dhcp l2relay circuit-id vlan` *`vlan-range`*

Mode Privileged EXEC

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

```
(Routing) #show dhcp l2relay circuit-id vlan 300

DHCP L2 Relay is  Enabled.

DHCP Circuit-Id option is enabled on the following VLANs:
300
```

show dhcp l2relay remote-id vlan

This command shows whether DHCP L2 Relay is globally enabled and shows the remote ID configured on the specified VLAN or range of VLANs.

Format `show dhcp l2relay remote-id vlan` *`vlan-range`*

Mode Privileged EXEC

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

```
(Routing) #show dhcp l2relay remote-id vlan 200

DHCP L2 Relay is  Enabled.

 VLAN ID   Remote Id
---------  -------------
200        remote_22
```

clear dhcp l2relay statistics interface

Use this command to reset the DHCP L2 relay counters to zero. Specify the port with the counters to clear, or use the `all` keyword to clear the counters on all ports.

Format `clear dhcp l2relay statistics interface {slot/port | all}`

Mode Privileged EXEC

DHCP Client Commands

DWS-4000 can include vendor and configuration information in DHCP client requests relayed to a DHCP server. This information is included in DHCP Option 60, Vendor Class Identifier. The information is a string of 128 octets.

dhcp client vendor-id-option

This command enables the inclusion of DHCP Option-60, Vendor Class Identifier included in the requests transmitted to the DHCP server by the DHCP client operating in the DWS-4000 switch.

Format `dhcp client vendor-id-option` *`string`*

Mode Global Config

no dhcp client vendor-id-option

This command disables the inclusion of DHCP Option-60, Vendor Class Identifier included in the requests transmitted to the DHCP server by the DHCP client operating in the DWS-4000 switch.

Format `no dhcp client vendor-id-option`

Mode Global Config

dhcp client vendor-id-option-string

This parameter sets the DHCP Vendor Option-60 string to be included in the requests transmitted to the DHCP server by the DHCP client operating in the DWS-4000 switch.

Format `dhcp client vendor-id-option-string` *`string`*

Mode Global Config

no dhcp client vendor-id-option-string

This parameter clears the DHCP Vendor Option-60 string.

Format `no dhcp client vendor-id-option-string`

Mode Global Config

show dhcp client vendor-id-option

This command displays the configured administration mode of the vendor-id-option and the vendor-id string to be included in Option-43 in DHCP requests.

Format `show dhcp client vendor-id-option`

Mode Privileged EXEC

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

```
(Switching) #show dhcp client vendor-id-option

DHCP Client Vendor Identifier Option is Enabled
DHCP Client Vendor Identifier Option string is FastpathClient.
```

DHCP Snooping Configuration Commands

This section describes commands you use to configure DHCP Snooping.

ip dhcp snooping

Use this command to enable DHCP Snooping globally.

Default disabled
Format `ip dhcp snooping`
Mode Global Config

no ip dhcp snooping

Use this command to disable DHCP Snooping globally.

Format `no ip dhcp snooping`
Mode Global Config

ip dhcp snooping vlan

Use this command to enable DHCP Snooping on a list of comma-separated VLAN ranges.

Default disabled
Format `ip dhcp snooping vlan` *`vlan-list`*
Mode Global Config

no ip dhcp snooping vlan

Use this command to disable DHCP Snooping on VLANs.

Format `no ip dhcp snooping vlan` *`vlan-list`*
Mode Global Config

ip dhcp snooping verify mac-address

Use this command to enable verification of the source MAC address with the client hardware address in the received DCHP message.

Default enabled

Format `ip dhcp snooping verify mac-address`

Mode Global Config

no ip dhcp snooping verify mac-address

Use this command to disable verification of the source MAC address with the client hardware address.

Format `no ip dhcp snooping verify mac-address`

Mode Global Config

ip dhcp snooping database

Use this command to configure the persistent location of the DHCP Snooping database. This can be local or a remote file on a given IP machine.

Default local

Format `ip dhcp snooping database {local|tftp://hostIP/filename}`

Mode Global Config

ip dhcp snooping database write-delay

Use this command to configure the interval in seconds at which the DHCP Snooping database will be persisted. The interval value ranges from 15 to 86400 seconds.

Default 300 seconds

Format `ip dhcp snooping database write-delay in seconds`

Mode Global Config

no ip dhcp snooping database write-delay

Use this command to set the write delay value to the default value.

Format `no ip dhcp snooping database write-delay`

Mode Global Config

ip dhcp snooping binding

Use this command to configure static DHCP Snooping binding.

Format `ip dhcp snooping binding mac-address vlan vlan id ip address interface interface id`

Mode Global Config

no ip dhcp snooping binding

Use this command to remove the DHCP static entry from the DHCP Snooping database.

Format `no ip dhcp snooping binding mac-address`

Mode Global Config

ip verify binding

Use this command to configure static IP source guard (IPSG) entries.

Format `ip verify binding mac-address vlan vlan id ip address interface interface id`

Mode Global Config

no ip verify binding

Use this command to remove the IPSG static entry from the IPSG database.

Format `no ip verify binding mac-address vlan vlan id ip address interface interface id`

Mode Global Config

ip dhcp snooping limit

Use this command to control the rate at which the DHCP Snooping messages come on an interface or range of interfaces. By default, rate limiting is disabled. When enabled, the rate can range from 0 to 30 packets per second. The burst level range is 1 to 15 seconds.

Default disabled (no limit)

Format `ip dhcp snooping limit {rate pps [burst interval seconds]}`

Mode Interface Config

no ip dhcp snooping limit

Use this command to set the rate at which the DHCP Snooping messages come, and the burst level, to the defaults.

Format `no ip dhcp snooping limit`

Mode Interface Config

ip dhcp snooping log-invalid

Use this command to control the logging DHCP messages filtration by the DHCP Snooping application. This command can be used to configure a single interface or a range of interfaces.

Default disabled

Format `ip dhcp snooping log-invalid`

Mode Interface Config

no ip dhcp snooping log-invalid

Use this command to disable the logging DHCP messages filtration by the DHCP Snooping application.

Format `no ip dhcp snooping log-invalid`

Mode Interface Config

ip dhcp snooping trust

Use this command to configure an interface or range of interfaces as trusted.

Default disabled

Format `ip dhcp snooping trust`

Mode Interface Config

no ip dhcp snooping trust

Use this command to configure the port as untrusted.

Format `no ip dhcp snooping trust`

Mode Interface Config

ip verify source

Use this command to configure the IPSG source ID attribute to filter the data traffic in the hardware. Source ID is the combination of IP address and MAC address. Normal command allows data traffic filtration based on the IP address. With the `port-security` option, the data traffic will be filtered based on the IP and MAC addresses.

This command can be used to configure a single interface or a range of interfaces.

Default `the source ID is the IP address`

Format `ip verify source {port-security}`

Mode Interface Config

no ip verify source

Use this command to disable the IPSG configuration in the hardware. You cannot disable port-security alone if it is configured.

Format `no ip verify source`

Mode Interface Config

show ip dhcp snooping

Use this command to display the DHCP Snooping global configurations and per port configurations.

Format `show ip dhcp snooping`

Mode
- Privileged EXEC
- User EXEC

Term	*Definition*
Interface	The interface for which data is displayed.
Trusted	If it is enabled, DHCP snooping considers the port as trusted. The factory default is disabled.
Log Invalid Pkts	If it is enabled, DHCP snooping application logs invalid packets on the specified interface.

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

```
(switch) #show ip dhcp snooping

DHCP snooping is Disabled
DHCP snooping source MAC verification is enabled
DHCP snooping is enabled on the following VLANs:
11 - 30, 40

Interface   Trusted    Log Invalid Pkts
---------   --------   ----------------
0/1          Yes             No
0/2          No             Yes
```

```
0/3          No              Yes
0/4          No               No
0/6          No               No
```

show ip dhcp snooping binding

Use this command to display the DHCP Snooping binding entries. To restrict the output, use the following options:

- Dynamic: Restrict the output based on DCHP snooping.
- Interface: Restrict the output based on a specific interface.
- Static: Restrict the output based on static entries.
- VLAN: Restrict the output based on VLAN.

Format `show ip dhcp snooping binding [{static/dynamic}] [interface slot/port] [vlan id]`

Mode
- Privileged EXEC
- User EXEC

Term	*Definition*
MAC Address	Displays the MAC address for the binding that was added. The MAC address is the key to the binding database.
IP Address	Displays the valid IP address for the binding rule.
VLAN	The VLAN for the binding rule.
Interface	The interface to add a binding into the DHCP snooping interface.
Type	Binding type; statically configured from the CLI or dynamically learned.
Lease (sec)	The remaining lease time for the entry.

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

```
(switch) #show ip dhcp snooping binding

Total number of bindings: 2

MAC Address          IP Address   VLAN  Interface  Type  Lease time (Secs)
------------------  ------------  ----  ---------  ---- ------------------
00:02:B3:06:60:80   210.1.1.3      10   0/1                  86400
00:0F:FE:00:13:04   210.1.1.4      10   0/1                  86400
```

show ip dhcp snooping database

Use this command to display the DHCP Snooping configuration related to the database persistency.

Format `show ip dhcp snooping database`

Mode
- Privileged EXEC
- User EXEC

Term	*Definition*
Agent URL	Bindings database agent URL.
Write Delay	The maximum write time to write the database into local or remote.

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

```
(switch) #show ip dhcp snooping database

agent url:  /10.131.13.79:/sai1.txt

write-delay:  5000
```

show ip dhcp snooping interfaces

Use this command to show the DHCP Snooping status of the interfaces.

Format `show ip dhcp snooping interfaces`

Mode Privileged EXEC

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

```
(switch) #show ip dhcp snooping interfaces

 Interface    Trust State    Rate Limit     Burst Interval
                                (pps)       (seconds)
-----------   ----------   ----------   --------------
    1/g1             No            15                1
    1/g2             No            15                1
    1/g3             No            15                1

(switch) #show ip dhcp snooping interfaces ethernet 1/g15

 Interface    Trust State    Rate Limit     Burst Interval
                                (pps)       (seconds)
-----------   ----------   ----------   --------------
    1/g15            Yes           15                1
```

show ip dhcp snooping statistics

Use this command to list statistics for DHCP Snooping security violations on untrusted ports.

Format `show ip dhcp snooping statistics`

Mode
- Privileged EXEC
- User EXEC

Term	*Definition*
Interface	The IP address of the interface in slot/port format.
MAC Verify Failures	Represents the number of DHCP messages that were filtered on an untrusted interface because of source MAC address and client HW address mismatch.
Client Ifc Mismatch	Represents the number of DHCP release and Deny messages received on the different ports than learned previously.
DHCP Server Msgs Rec'd	Represents the number of DHCP server messages received on Untrusted ports.

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

```
(switch) #show ip dhcp snooping statistics

 Interface    MAC Verify   Client Ifc   DHCP Server
               Failures     Mismatch    Msgs Rec'd
-----------   ----------   ----------   -----------
1/0/2                 0            0             0
1/0/3                 0            0             0
1/0/4                 0            0             0
1/0/5                 0            0             0
1/0/6                 0            0             0
1/0/7                 0            0             0
1/0/8                 0            0             0
1/0/9                 0            0             0
1/0/10                0            0             0
1/0/11                0            0             0
1/0/12                0            0             0
1/0/13                0            0             0
1/0/14                0            0             0
1/0/15                0            0             0
1/0/16                0            0             0
1/0/17                0            0             0
1/0/18                0            0             0
1/0/19                0            0             0
1/0/20                0            0             0
```

clear ip dhcp snooping binding

Use this command to clear all DHCP Snooping bindings on all interfaces or on a specific interface.

Format `clear ip dhcp snooping binding [interface slot/port]`

Mode
- Privileged EXEC
- User EXEC

clear ip dhcp snooping statistics

Use this command to clear all DHCP Snooping statistics.

Format `clear ip dhcp snooping statistics`

Mode
- Privileged EXEC
- User EXEC

show ip verify source

Use this command to display the IPSG configurations on all ports.

Format `show ip verify source`

Mode
- Privileged EXEC
- User EXEC

Term	*Definition*
Interface	Interface address in slot/port format.
Filter Type	Is one of two values: • ip-mac: User has configured MAC address filtering on this interface. • ip: Only IP address filtering on this interface.
IP Address	IP address of the interface
MAC Address	If MAC address filtering is not configured on the interface, the MAC Address field is empty. If port security is disabled on the interface, then the MAC Address field displays `permit-all`.
VLAN	The VLAN for the binding rule.

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

```
(switch) #show ip verify source

Interface  Filter Type    IP Address       MAC Address      Vlan
---------  -----------  ---------------  -----------------  -----
    0/1     ip-mac       210.1.1.3       00:02:B3:06:60:80     10
    0/1     ip-mac       210.1.1.4       00:0F:FE:00:13:04     10
```

show ip verify interface

Use this command to display the IPSG filter type for a specific interface.

Format `show ip verify interface slot/port`

Mode
- Privileged EXEC
- User EXEC

Term	*Definition*
Interface	Interface address in slot/port format.
Filter Type	Is one of two values: • ip-mac: User has configured MAC address filtering on this interface. • ip: Only IP address filtering on this interface.

show ip source binding

Use this command to display the IPSG bindings.

Format `show ip source binding [{static/dynamic}] [interface slot/port] [vlan id]`

Mode
- Privileged EXEC
- User EXEC

Term	*Definition*
MAC Address	The MAC address for the entry that is added.
IP Address	The IP address of the entry that is added.
Type	Entry type; statically configured from CLI or dynamically learned from DHCP Snooping.
VLAN	VLAN for the entry.
Interface	IP address of the interface in slot/port format.

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

```
(switch) #show ip source binding

MAC Address       IP Address       Type          Vlan     Interface
----------------  ---------------  ------------  -----  -------------
00:00:00:00:00:08          1.2.3.4  dhcp-snooping     2        1/0/1
00:00:00:00:00:09          1.2.3.4  dhcp-snooping     3        1/0/1
00:00:00:00:00:0A          1.2.3.4  dhcp-snooping     4        1/0/1
```

Dynamic ARP Inspection Commands

Dynamic ARP Inspection (DAI) is a security feature that rejects invalid and malicious ARP packets. DAI prevents a class of man-in-the-middle attacks, where an unfriendly station intercepts traffic for other stations by poisoning the ARP caches of its unsuspecting neighbors. The miscreant sends ARP requests or responses mapping another station's IP address to its own MAC address.

DAI relies on DHCP snooping. DHCP snooping listens to DHCP message exchanges and builds a binding database of valid {MAC address, IP address, VLAN, and interface} tuples.

When DAI is enabled, the switch drops ARP packets whose sender MAC address and sender IP address do not match an entry in the DHCP snooping bindings database. You can optionally configure additional ARP packet validation.

ip arp inspection vlan

Use this command to enable Dynamic ARP Inspection on a list of comma-separated VLAN ranges.

Default `disabled`

Format `ip arp inspection vlan vlan-list`

Mode Global Config

no ip arp inspection vlan

Use this command to disable Dynamic ARP Inspection on a list of comma-separated VLAN ranges.

Format `no ip arp inspection vlan vlan-list`

Mode Global Config

ip arp inspection validate

Use this command to enable additional validation checks like source-mac validation, destination-mac validation, and ip address validation on the received ARP packets. Each command overrides the configuration of the previous command. For example, if a command enables src-mac and dst-mac validations, and a second command enables IP validation only, the src-mac and dst-mac validations are disabled as a result of the second command.

Default `disabled`

Format `ip arp inspection validate {[src-mac] [dst-mac] [ip]}`

Mode Global Config

no ip arp inspection validate

Use this command to disable the additional validation checks on the received ARP packets.

Format `no ip arp inspection validate {[src-mac] [dst-mac] [ip]}`

Mode Global Config

ip arp inspection vlan logging

Use this command to enable logging of invalid ARP packets on a list of comma-separated VLAN ranges.

Default `enabled`

Format `ip arp inspection vlan vlan-list logging`

Mode Global Config

no ip arp inspection vlan logging

Use this command to disable logging of invalid ARP packets on a list of comma-separated VLAN ranges.

Format `no ip arp inspection vlan vlan-list logging`

Mode Global Config

ip arp inspection trust

Use this command to configure an interface or range of interfaces as trusted for Dynamic ARP Inspection.

Default `enabled`

Format `ip arp inspection trust`

Mode Interface Config

no ip arp inspection trust

Use this command to configure an interface as untrusted for Dynamic ARP Inspection.

Format `no ip arp inspection trust`

Mode Interface Config

ip arp inspection limit

Use this command to configure the rate limit and burst interval values for an interface or range of interfaces. Configuring none for the limit means the interface is not rate limited for Dynamic ARP Inspections. The maximum pps value shown in the range for the rate option might be more than the hardware allowable limit. Therefore you need to understand the switch performance and configure the maximum rate pps accordingly.

Note: The user interface will accept a rate limit for a trusted interface, but the limit will not be enforced unless the interface is configured to be untrusted.

Default `15 pps for rate and 1 second for burst-interval`

Format `ip arp inspection limit {rate pps [burst interval seconds] | none}`

Mode Interface Config

no ip arp inspection limit

Use this command to set the rate limit and burst interval values for an interface to the default values of 15 pps and 1 second, respectively.

Format `no ip arp inspection limit`

Mode Interface Config

ip arp inspection filter

Use this command to configure the ARP ACL used to filter invalid ARP packets on a list of comma-separated VLAN ranges. If the static keyword is given, packets that do not match a permit statement are dropped without consulting the DHCP snooping bindings.

Default `No ARP ACL is configured on a VLAN`

Format `ip arp inspection filter acl-name vlan vlan-list [static]`

Mode Global Config

no ip arp inspection filter

Use this command to unconfigure the ARP ACL used to filter invalid ARP packets on a list of comma-separated VLAN ranges.

Format `no ip arp inspection filter acl-name vlan vlan-list [static]`

Mode Global Config

arp access-list

Use this command to create an ARP ACL.

Format `arp access-list acl-name`

Mode Global Config

no arp access-list

Use this command to delete a configured ARP ACL.

Format `no arp access-list acl-name`

Mode Global Config

permit ip host mac host

Use this command to configure a rule for a valid IP address and MAC address combination used in ARP packet validation.

Format `permit ip host sender-ip mac host sender-mac`

Mode ARP Access-list Config

no permit ip host mac host

Use this command to delete a rule for a valid IP and MAC combination.

Format `no permit ip host sender-ip mac host sender-mac`

Mode ARP Access-list Config

show ip arp inspection

Use this command to display the Dynamic ARP Inspection global configuration and configuration on all the VLANs. With the *vlan-list* argument (i.e. comma separated VLAN ranges), the command displays the global configuration and configuration on all the VLANs in the given VLAN list. The global configuration includes the **source mac validation**, **destination mac validation** and **invalid IP validation** information.

Format `show ip arp inspection [vlan vlan-list]`

Mode
- Privileged EXEC
- User EXEC

Term	*Definition*
Source MAC Validation	Displays whether Source MAC Validation of ARP frame is enabled or disabled.
Destination MAC Validation	Displays whether Destination MAC Validation is enabled or disabled.
IP Address Validation	Displays whether IP Address Validation is enabled or disabled.
VLAN	The VLAN ID for each displayed row.
Configuration	Displays whether DAI is enabled or disabled on the VLAN.
Log Invalid	Displays whether logging of invalid ARP packets is enabled on the VLAN.
ACL Name	The ARP ACL Name, if configured on the VLAN.
Static Flag	If the ARP ACL is configured static on the VLAN.

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

```
(switch) #show ip arp inspection vlan 10-12

Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled

 Vlan          Configuration    Log Invalid   ACL Name   Static flag
 ----          -------------    -----------   ---------  ----------
   10               Enabled        Enabled   H2         Enabled
   11              Disabled        Enabled
   12               Enabled       Disabled
```

show ip arp inspection statistics

Use this command to display the statistics of the ARP packets processed by Dynamic ARP Inspection. Give the vlan-list argument and the command displays the statistics on all DAI-enabled VLANs in that list. Give the single vlan argument and the command displays the statistics on that VLAN. If no argument is included, the command lists a summary of the forwarded and dropped ARP packets.

Format `show ip arp inspection statistics [vlan vlan-list]`

Mode
- Privileged EXEC
- User EXEC

Term	*Definition*
VLAN	The VLAN ID for each displayed row.
Forwarded	The total number of valid ARP packets forwarded in this VLAN.
Dropped	The total number of not valid ARP packets dropped in this VLAN.
DHCP Drops	The number of packets dropped due to DHCP snooping binding database match failure.
ACL Drops	The number of packets dropped due to ARP ACL rule match failure.
DHCP Permits	The number of packets permitted due to DHCP snooping binding database match.
ACL Permits	The number of packets permitted due to ARP ACL rule match.
Bad Src MAC	The number of packets dropped due to Source MAC validation failure.
Bad Dest MAC	The number of packets dropped due to Destination MAC validation failure.
Invalid IP	The number of packets dropped due to invalid IP checks.

Example: The following shows example CLI display output for the command **show ip arp inspection statistics** which lists the summary of forwarded and dropped ARP packets on all DAI-enabled VLANs.

```
VLAN  Forwarded  Dropped
----  ---------  -------
  10         90       14
  20         10        3
```

Example: The following shows example CLI display output for the command `show ip arp inspection statistics vlan` *`vlan-list`*.

```
VLAN    DHCP       ACL        DHCP        ACL        Bad Src    Bad Dest    Invalid
         Drops      Drops       Permits     Permits       MAC        MAC         IP
----- -------- --------- ----------- --------- ---------- ----------- ---------
10       11          1             65          25             1           1          0
20       1           0              8           2             0           1          1
```

clear ip arp inspection statistics

Use this command to reset the statistics for Dynamic ARP Inspection on all VLANs.

Default none

Format `clear ip arp inspection statistics`

Mode Privileged EXEC

show ip arp inspection interfaces

Use this command to display the Dynamic ARP Inspection configuration on all the DAI-enabled interfaces. An interface is said to be enabled for DAI if at least one VLAN, that the interface is a member of, is enabled for DAI. Given a slot/port interface argument, the command displays the values for that interface whether the interface is enabled for DAI or not.

Format `show ip arp inspection interfaces [slot/port]`

Mode
- Privileged EXEC
- User EXEC

Term	*Definition*
Interface	The interface ID for each displayed row.
Trust State	Whether the interface is trusted or untrusted for DAI.
Rate Limit	The configured rate limit value in packets per second.
Burst Interval	The configured burst interval value in seconds.

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

```
(switch) #show ip arp inspection interfaces

 Interface        Trust State   Rate Limit   Burst Interval
                                   (pps)        (seconds)
 ---------------  -----------   ----------  ---------------
 0/1                Untrusted           15                1
 0/2                Untrusted           10               10
```

show arp access-list

Use this command to display the configured ARP ACLs with the rules. Giving an ARP ACL name as the argument will display only the rules in that ARP ACL.

Format `show arp access-list [acl-name]`

Mode
- Privileged EXEC
- User EXEC

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

```
(switch) #show arp access-list

ARP access list H2
    permit ip host 1.1.1.1 mac host 00:01:02:03:04:05
    permit ip host 1.1.1.2 mac host 00:03:04:05:06:07
ARP access list H3
ARP access list H4
    permit ip host 2.1.1.2 mac host 00:03:04:05:06:08
```

IGMP Snooping Configuration Commands

This section describes the commands you use to configure IGMP snooping. DWS-4000 software supports IGMP Versions 1, 2, and 3. The IGMP snooping feature can help conserve bandwidth because it allows the switch to forward IP multicast traffic only to connected hosts that request multicast traffic. IGMPv3 adds source filtering capabilities to IGMP versions 1 and 2.

set igmp

This command enables IGMP Snooping on the system (Global Config Mode), an interface, or a range of interfaces. This command also enables IGMP snooping on a particular VLAN (VLAN Config Mode) and can enable IGMP snooping on all interfaces participating in a VLAN.

If an interface has IGMP Snooping enabled and you enable this interface for routing or enlist it as a member of a port-channel (LAG), IGMP Snooping functionality is disabled on that interface. IGMP Snooping functionality is re-enabled if you disable routing or remove port-channel (LAG) membership from an interface that has IGMP Snooping enabled.

The IGMP application supports the following activities:

- Validation of the IP header checksum (as well as the IGMP header checksum) and discarding of the frame upon checksum error.
- Maintenance of the forwarding table entries based on the MAC address versus the IP address.
- Flooding of unregistered multicast data packets to all ports in the VLAN.

Default disabled

Format `set igmp [vlan_id]`

Mode
- Global Config
- Interface Config
- VLAN Config

no set igmp

This command disables IGMP Snooping on the system, an interface, a range of interfaces, or a VLAN.

Format `no set igmp [vlan_id]`

Mode
- Global Config
- Interface Config
- VLAN Config

set igmp interfacemode

This command enables IGMP Snooping on all interfaces. If an interface has IGMP Snooping enabled and you enable this interface for routing or enlist it as a member of a port-channel (LAG), IGMP Snooping functionality is disabled on that interface. IGMP Snooping functionality is re-enabled if you disable routing or remove port-channel (LAG) membership from an interface that has IGMP Snooping enabled.

Default disabled

Format `set igmp interfacemode`

Mode Global Config

no set igmp interfacemode

This command disables IGMP Snooping on all interfaces.

Format `no set igmp interfacemode`

Mode Global Config

set igmp fast-leave

This command enables or disables IGMP Snooping fast-leave admin mode on a selected interface, a range of interfaces, or a VLAN. Enabling fast-leave allows the switch to immediately remove the layer 2 LAN interface from its forwarding table entry upon receiving an IGMP leave message for that multicast group without first sending out MAC-based general queries to the interface.

You should enable fast-leave admin mode only on VLANs where only one host is connected to each layer 2 LAN port. This prevents the inadvertent dropping of the other hosts that were connected to the same layer 2 LAN port but were still interested in receiving multicast traffic directed to that group. Also, fast-leave processing is supported only with IGMP version 2 hosts.

Default disabled

Format `set igmp fast-leave [vlan_id]`

Mode Interface Config
Interface Range
VLAN Config

no set igmp fast-leave

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

Format `no set igmp fast-leave [vlan_id]`

Mode Interface Config
Interface Range
VLAN Config

set igmp groupmembership-interval

This command sets the IGMP Group Membership Interval time on a VLAN, one interface, a range of interfaces, or all interfaces. The Group Membership Interval time is the amount of time in seconds that a switch waits for a report from a particular group on a particular interface before deleting the interface from the entry. This value must be greater than the IGMPv3 Maximum Response time value. The range is 2 to 3600 seconds.

Default 260 seconds

Format `set igmp groupmembership-interval [vlan_id] 2—3600`

Mode
- Interface Config
- Global Config
- VLAN Config

no set igmp groupmembership-interval

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

Format `no set igmp groupmembership-interval [vlan_id]`

Mode
- Interface Config
- Global Config
- VLAN Config

set igmp maxresponse

This command sets the IGMP Maximum Response time for the system, on a particular interface or VLAN, or on a range of interfaces. The Maximum Response time is the amount of time in seconds that a switch will wait after sending a query on an interface because it did not receive a report for a particular group in that interface. This value must be less than the IGMP Query Interval time value. The range is 1 to 25 seconds.

Default 10 seconds

Format `set igmp maxresponse [vlan_id] 1—25`

Mode
- Global Config
- Interface Config
- VLAN Config

no set igmp maxresponse

This command sets the max response time (on the interface or VLAN) to the default value.

Format `no set igmp maxresponse [vlan_id]`

Mode
- Global Config
- Interface Config
- VLAN Config

set igmp mcrtrexpiretime

This command sets the Multicast Router Present Expiration time. The time is set for the system, on a particular interface or VLAN, or on a range of interfaces. This is the amount of time in seconds that a switch waits for a query to be received on an interface before the interface is removed from the list of interfaces with multicast routers attached. The range is 0 to 3600 seconds. A value of 0 indicates an infinite time-out, i.e. no expiration.

Default 0

Format `set igmp mcrtrexpiretime [vlan_id] 0—3600`

Mode
- Global Config
- Interface Config
- VLAN Config

no set igmp mcrtrexpiretime

This command sets the Multicast Router Present Expiration time to 0. The time is set for the system, on a particular interface or a VLAN.

Format `no set igmp mcrtrexpiretime [vlan_id]`

Mode
- Global Config
- Interface Config
- VLAN Config

Format `no set igmp mcrtrexpiretime vlan_id`

Mode VLAN Config

set igmp mrouter

This command configures the VLAN ID (*vlan_id*) that has the multicast router mode enabled.

Format `set igmp mrouter vlan_id`

Mode Interface Config

no set igmp mrouter

This command disables multicast router mode for a particular VLAN ID (*vlan_id*).

Format `no set igmp mrouter vlan_id`

Mode Interface Config

set igmp mrouter interface

This command configures the interface or range of interfaces as a multicast router interface. When configured as a multicast router interface, the interface is treated as a multicast router interface in all VLANs.

Default disabled

Format `set igmp mrouter interface`

Mode Interface Config

no set igmp mrouter interface

This command disables the status of the interface as a statically configured multicast router interface.

Format `no set igmp mrouter interface`

Mode Interface Config

show igmpsnooping

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

Format `show igmpsnooping [slot/port | vlan_id]`

Mode Privileged EXEC

When the optional arguments slot/port or *vlan_id* are not used, the command displays the following information:

Term	*Definition*
Admin Mode	Indicates whether or not IGMP Snooping is active on the switch.
Multicast Control Frame Count	The number of multicast control frames that are processed by the CPU.
Interface Enabled for IGMP Snooping	The list of interfaces on which IGMP Snooping is enabled.
VLANS Enabled for IGMP Snooping	The list of VLANS on which IGMP Snooping is enabled.

When you specify the slot/port values, the following information appears:

Term	*Definition*
IGMP Snooping Admin Mode	Indicates whether IGMP Snooping is active on the interface.
Fast Leave Mode	Indicates whether IGMP Snooping Fast-leave is active on the interface.
Group Membership Interval	The amount of time in seconds that a switch will wait for a report from a particular group on a particular interface before deleting the interface from the entry.This value may be configured.
Maximum Response Time	The amount of time the switch waits after it sends a query on an interface because it did not receive a report for a particular group on that interface. This value may be configured.
Multicast Router Expiry Time	The amount of time to wait before removing an interface from the list of interfaces with multicast routers attached. The interface is removed if a query is not received. This value may be configured.

When you specify a value for *vlan_id*, the following information appears:

Term	*Definition*
VLAN ID	The VLAN ID.
IGMP Snooping Admin Mode	Indicates whether IGMP Snooping is active on the VLAN.
Fast Leave Mode	Indicates whether IGMP Snooping Fast-leave is active on the VLAN.
Group Membership Interval	The amount of time in seconds that a switch will wait for a report from a particular group on a particular interface, which is participating in the VLAN, before deleting the interface from the entry.This value may be configured.
Maximum Response Time	The amount of time the switch waits after it sends a query on an interface, participating in the VLAN, because it did not receive a report for a particular group on that interface. This value may be configured.
Multicast Router Expiry Time	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.

show igmpsnooping mrouter interface

This command displays information about statically configured ports.

Format `show igmpsnooping mrouter interface slot/port`

Mode Privileged EXEC

Term	*Definition*
Interface	The port on which multicast router information is being displayed.
Multicast Router Attached	Indicates whether multicast router is statically enabled on the interface.
VLAN ID	The list of VLANs of which the interface is a member.

show igmpsnooping mrouter vlan

This command displays information about statically configured ports.

Format `show igmpsnooping mrouter vlan slot/port`

Mode Privileged EXEC

Term	*Definition*
Interface	The port on which multicast router information is being displayed.
VLAN ID	The list of VLANs of which the interface is a member.

show mac-address-table igmpsnooping

This command displays the IGMP Snooping entries in the MFDB table.

Format `show mac-address-table igmpsnooping`

Mode Privileged EXEC

Term	*Definition*
VLAN ID	The VLAN in which the MAC address is learned.
MAC Address	A multicast MAC address for which the switch has forwarding or filtering information. The format is 6 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB.
Type	The type of the entry, which is either static (added by the user) or dynamic (added to the table as a result of a learning process or protocol).
Description	The text description of this multicast table entry.
Interfaces	The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).

IGMP Snooping Querier Commands

IGMP Snooping requires that one central switch or router periodically query all end-devices on the network to announce their multicast memberships. This central device is the IGMP Querier. The IGMP query responses, known as IGMP reports, keep the switch updated with the current multicast group membership on a port-by-port basis. If the switch does not receive updated membership information in a timely fashion, it will stop forwarding multicasts to the port where the end device is located.

This section describes commands used to configure and display information on IGMP Snooping Queriers on the network and, separately, on VLANs.

set igmp querier

Use this command to enable IGMP Snooping Querier on the system, using Global Config mode, or on a VLAN. Using this command, you can specify the IP Address that the Snooping Querier switch should use as the source address while generating periodic queries.

If a VLAN has IGMP Snooping Querier enabled and IGMP Snooping is operationally disabled on it, IGMP Snooping Querier functionality is disabled on that VLAN. IGMP Snooping functionality is re-enabled if IGMP Snooping is operational on the VLAN.

Note: The Querier IP Address assigned for a VLAN takes preference over global configuration.

The IGMP Snooping Querier application supports sending periodic general queries on the VLAN to solicit membership reports.

Default disabled

Format `set igmp querier [vlan-id] [address ipv4_address]`

Mode
- Global Config
- VLAN Mode

no set igmp querier

Use this command to disable IGMP Snooping Querier on the system. Use the optional `address` parameter to reset the querier address to 0.0.0.0.

Format `no set igmp querier [vlan-id] [address]`

Mode
- Global Config
- VLAN Mode

set igmp querier query-interval

Use this command to set the IGMP Querier Query Interval time. It is the amount of time in seconds that the switch waits before sending another general query.

Default disabled

Format `set igmp querier query-interval 1—18000`

Mode Global Config

no set igmp querier query-interval

Use this command to set the IGMP Querier Query Interval time to its default value.

Format `no set igmp querier query-interval`

Mode Global Config

set igmp querier timer expiry

Use this command to set the IGMP Querier timer expiration period. It is the time period that the switch remains in Non-Querier mode once it has discovered that there is a Multicast Querier in the network.

Default 60 seconds

Format `set igmp querier timer expiry 60—300`

Mode Global Config

no set igmp querier timer expiry

Use this command to set the IGMP Querier timer expiration period to its default value.

Format `no set igmp querier timer expiry`

Mode Global Config

set igmp querier version

Use this command to set the IGMP version of the query that the snooping switch is going to send periodically.

Default 1

Format `set igmp querier version 1—2`

Mode Global Config

no set igmp querier version

Use this command to set the IGMP Querier version to its default value.

Format `no set igmp querier version`

Mode Global Config

set igmp querier election participate

Use this command to enable the Snooping Querier to participate in the Querier Election process when it discovers the presence of another Querier in the VLAN. When this mode is enabled, if the Snooping Querier finds that the other Querier's source address is better (less) than the Snooping Querier's address, it stops sending periodic queries. If the Snooping Querier wins the election, then it will continue sending periodic queries.

Default disabled

Format `set igmp querier election participate`

Mode VLAN Config

no set igmp querier election participate

Use this command to set the Snooping Querier not to participate in querier election but go into non-querier mode as soon as it discovers the presence of another querier in the same VLAN.

Format `no set igmp querier election participate`

Mode VLAN Config

show igmpsnooping querier

Use this command to display IGMP Snooping Querier information. Configured information is displayed whether or not IGMP Snooping Querier is enabled.

Format `show igmpsnooping querier [{detail | vlan vlanid}]`

Mode Privileged EXEC

When the optional argument *vlanid* is not used, the command displays the following information.

Field	*Description*
Admin Mode	Indicates whether or not IGMP Snooping Querier is active on the switch.
Admin Version	The version of IGMP that will be used while sending out the queries.

Field	*Description*
Querier Address	The IP Address which will be used in the IPv4 header while sending out IGMP queries. It can be configured using the appropriate command.
Query Interval	The amount of time in seconds that a Snooping Querier waits before sending out the periodic general query.
Querier Timeout	The amount of time to wait in the Non-Querier operational state before moving to a Querier state.

When you specify a value for *vlanid*, the following additional information appears.

Field	*Description*
VLAN Admin Mode	Indicates whether iGMP Snooping Querier is active on the VLAN.
VLAN Operational State	Indicates whether IGMP Snooping Querier is in Querier" or Non-Querier" state. When the switch is in Querier state, it will send out periodic general queries. When in Non-Querier state, it will wait for moving to Querier state and does not send out any queries.
VLAN Operational Max Response Time	Indicates the time to wait before removing a Leave from a host upon receiving a Leave request. This value is calculated dynamically from the Queries received from the network. If the Snooping Switch is in Querier state, then it is equal to the configured value.
Querier Election Participation	Indicates whether the IGMP Snooping Querier participates in querier election if it discovers the presence of a querier in the VLAN.
Querier VLAN Address	The IP address will be used in the IPv4 header while sending out IGMP queries on this VLAN. It can be configured using the appropriate command.
Operational Version	The version of IPv4 will be used while sending out IGMP queries on this VLAN.
Last Querier Address	Indicates the IP address of the most recent Querier from which a Query was received.
Last Querier Version	Indicates the IGMP version of the most recent Querier from which a Query was received on this VLAN.

When the optional argument `detail` is used, the command shows the global information and the information for all Querier-enabled VLANs.

MLD Snooping Commands

This section describes commands used for MLD Snooping. In IPv4, Layer 2 switches can use IGMP Snooping to limit the flooding of multicast traffic by dynamically configuring Layer 2 interfaces so that multicast traffic is forwarded only to those interfaces associated with IP multicast addresses. In IPv6, MLD Snooping performs a similar function. With MLD Snooping, IPv6 multicast data is selectively forwarded to a list of ports that want to receive the data, instead of being flooded to all ports in a VLAN. This list is constructed by snooping IPv6 multicast control packets.

set mld

This command enables MLD Snooping on the system (Global Config Mode) or an Interface (Interface Config Mode). This command also enables MLD Snooping on a particular VLAN and enables MLD Snooping on all interfaces participating in a VLAN.

If an interface has MLD Snooping enabled and you enable this interface for routing or enlist it as a member of a port-channel (LAG), MLD Snooping functionality is disabled on that interface. MLD Snooping functionality is re-enabled if you disable routing or remove port channel (LAG) membership from an interface that has MLD Snooping enabled.

MLD Snooping supports the following activities:

- Validation of address version, payload length consistencies and discarding of the frame upon error.
- Maintenance of the forwarding table entries based on the MAC address versus the IPv6 address.
- Flooding of unregistered multicast data packets to all ports in the VLAN.

Default disabled

Format `set mld vlanid`

Mode
- Global Config
- Interface Config
- VLAN Mode

no set mld

Use this command to disable MLD Snooping on the system.

Format `set mld vlanid`

Mode
- Global Config
- Interface Config
- VLAN Mode

set mld interfacemode

Use this command to enable MLD Snooping on all interfaces. If an interface has MLD Snooping enabled and you enable this interface for routing or enlist it as a member of a port-channel (LAG), MLD Snooping functionality is disabled on that interface. MLD Snooping functionality is re-enabled if you disable routing or remove port-channel (LAG) membership from an interface that has MLD Snooping enabled.

Default	disabled
Format	`set mld interfacemode`
Mode	Global Config

no set mld interfacemode

Use this command to disable MLD Snooping on all interfaces.

Format	`no set mld interfacemode`
Mode	Global Config

set mld fast-leave

Use this command to enable MLD Snooping fast-leave admin mode on a selected interface or VLAN. Enabling fast-leave allows the switch to immediately remove the Layer 2 LAN interface from its forwarding table entry upon receiving and MLD done message for that multicast group without first sending out MAC-based general queries to the interface.

Note: You should enable fast-leave admin mode only on VLANs where only one host is connected to each Layer 2 LAN port. This prevents the inadvertent dropping of the other hosts that were connected to the same layer 2 LAN port but were still interested in receiving multicast traffic directed to that group.

Note: Fast-leave processing is supported only with MLD version 1 hosts.

Default	disabled
Format	`set mld fast-leave` *`vlanid`*
Mode	• Interface Config • VLAN Mode

no set mld fast-leave

Use this command to disable MLD Snooping fast-leave admin mode on a selected interface.

Format `no set mld fast-leave vlanid`

Mode
- Interface Config
- VLAN Mode

set mld groupmembership-interval

Use this command to set the MLD Group Membership Interval time on a VLAN, one interface or all interfaces. The Group Membership Interval time is the amount of time in seconds that a switch waits for a report from a particular group on a particular interface before deleting the interface from the entry. This value must be greater than the MLDv2 Maximum Response time value. The range is 2 to 3600 seconds.

Default 260 seconds

Format `set mld groupmembership-interval vlanid 2–3600`

Mode
- Interface Config
- Global Config
- VLAN Mode

no set groupmembership-interval

Use this command to set the MLDv2 Group Membership Interval time to the default value.

Format `no set mld groupmembership-interval`

Mode
- Interface Config
- Global Config
- VLAN Mode

set mld maxresponse

Use this command to set the MLD Maximum Response time for the system, on a particular interface or VLAN. The Maximum Response time is the amount of time in seconds that a switch will wait after sending a query on an interface because it did not receive a report for a particular group in that interface. This value must be less than the MLD Query Interval time value. The range is 1 to 65 seconds.

Default 10 seconds

Format `set mld maxresponse 1–65`

Mode
- Global Config
- Interface Config
- VLAN Mode

no set mld maxresponse

Use this command to set the max response time (on the interface or VLAN) to the default value.

Format `no set mld maxresponse`

Mode
- Global Config
- Interface Config
- VLAN Mode

set mld mcrtexpiretime

Use this command to set the Multicast Router Present Expiration time. The time is set for the system, on a particular interface or VLAN. This is the amount of time in seconds that a switch waits for a query to be received on an interface before the interface is removed from the list of interfaces with multicast routers attached. The range is 0 to 3600 seconds. A value of 0 indicates an infinite timeout, i.e. no expiration.

Default 0

Format `set mld mcrtexpiretime` *`vlanid 0–3600`*

Mode
- Global Config
- Interface Config

no set mld mcrtexpiretime

Use this command to set the Multicast Router Present Expiration time to 0. The time is set for the system, on a particular interface or a VLAN.

Format `no set mld mcrtexpiretime` *`vlanid`*

Mode
- Global Config
- Interface Config

set mld mrouter

Use this command to configure the VLAN ID for the VLAN that has the multicast router attached mode enabled.

Format `set mld mrouter` *`vlanid`*

Mode Interface Config

no set mld mrouter

Use this command to disable multicast router attached mode for a VLAN with a particular VLAN ID.

Format `no set mld mrouter` *`vlanid`*

Mode Interface Config

set mld mrouter interface

Use this command to configure the interface as a multicast router-attached interface. When configured as a multicast router interface, the interface is treated as a multicast router-attached interface in all VLANs.

Default disabled

Format `set mld mrouter interface`

Mode Interface Config

no set mld mrouter interface

Use this command to disable the status of the interface as a statically configured multicast router-attached interface.

Format `no set mld mrouter interface`

Mode Interface Config

show mldsnooping

Use this command to display MLD Snooping information. Configured information is displayed whether or not MLD Snooping is enabled.

Format `show mldsnooping` *`[unit/slot/port | vlanid]`*

Mode Privileged EXEC

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

Term	*Definition*
Admin Mode	Indicates whether or not MLD Snooping is active on the switch.
Interfaces Enabled for MLD Snooping	Interfaces on which MLD Snooping is enabled.
MLD Control Frame Count	Displays the number of MLD Control frames that are processed by the CPU.
VLANs Enabled for MLD Snooping	VLANs on which MLD Snooping is enabled.

When you specify the *`unit/slot/port`* values, the following information displays.

Term	*Definition*
MLD Snooping Admin Mode	Indicates whether MLD Snooping is active on the interface.

Term	*Definition*
Fast Leave Mode	Indicates whether MLD Snooping Fast Leave is active on the VLAN.
Group Membership Interval	Shows the amount of time in seconds that a switch will wait for a report from a particular group on a particular interface, which is participating in the VLAN, before deleting the interface from the entry. This value may be configured.
Max Response Time	Displays the amount of time the switch waits after it sends a query on an interface, participating in the VLAN, because it did not receive a report for a particular group on that interface. This value may be configured.
Multicast Router Present Expiration Time	Displays the amount of time to wait before removing an interface that is participating in the VLAN from the list of interfaces with multicast routers attached. The interface is removed if a query is not received. This value may be configured.

When you specify a value for *vlanid*, the following information appears.

Term	*Definition*
VLAN Admin Mode	Indicates whether MLD Snooping is active on the VLAN.

show mldsnooping mrouter interface

Use this command to display information about statically configured multicast router attached interfaces.

Format `show mldsnooping mrouter interface` *unit/slot/port*

Mode Privileged EXEC

Term	*Definition*
Interface	Shows the interface on which multicast router information is being displayed.
Multicast Router Attached	Indicates whether multicast router is statically enabled on the interface.
VLAN ID	Displays the list of VLANs of which the interface is a member.

show mldsnooping mrouter vlan

Use this command to display information about statically configured multicast router-attached interfaces.

Format `show mldsnooping mrouter vlan` *unit/slot/port*

Mode Privileged EXEC

Term	*Definition*
Interface	Shows the interface on which multicast router information is being displayed.
VLAN ID	Displays the list of VLANs of which the interface is a member.

show mac-address-table mldsnooping

Use this command to display the MLD Snooping entries in the Multicast Forwarding Database (MFDB) table.

Format `show mac-address-table mldsnooping`

Mode Privileged EXEC

Term	*Definition*
VLAN ID	The VLAN in which the MAC address is learned.
MAC Address	A multicast MAC address for which the switch has forwarding or filtering information. The format is 6 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB.
Type	The type of entry, which is either static (added by the user) or dynamic (added to the table as a result of a learning process or protocol.)
Description	The text description of this multicast table entry.
Interfaces	The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).

clear mldsnooping

Use this command to delete all MLD snooping entries from the MFDB table.

Format `clear mldsnooping`

Mode Privileged EXEC

MLD Snooping Querier Commands

In an IPv6 environment, MLD Snooping requires that one central switch or router periodically query all end-devices on the network to announce their multicast memberships. This central device is the MLD Querier. The MLD query responses, known as MLD reports, keep the switch updated with the current multicast group membership on a port-by-port basis. If the switch does not receive updated membership information in a timely fashion, it will stop forwarding multicasts to the port where the end device is located.

This section describes the commands you use to configure and display information on MLD Snooping queries on the network and, separately, on VLANs.

set mld querier

Use this command to enable MLD Snooping Querier on the system (Global Config Mode) or on a VLAN. Using this command, you can specify the IP address that the snooping querier switch should use as a source address while generating periodic queries.

If a VLAN has MLD Snooping Querier enabled and MLD Snooping is operationally disabled on it, MLD Snooping Querier functionality is disabled on that VLAN. MLD Snooping functionality is re-enabled if MLD Snooping is operational on the VLAN.

The MLD Snooping Querier sends periodic general queries on the VLAN to solicit membership reports.

Default disabled

Format `set mld querier [vlan-id] [address ipv6_address]`

Mode
- Global Config
- VLAN Mode

no set mld querier

Use this command to disable MLD Snooping Querier on the system. Use the optional parameter `address` to reset the querier address.

Format `no set mld querier [vlan-id][address]`

Mode
- Global Config
- VLAN Mode

set mld querier query_interval

Use this command to set the MLD Querier Query Interval time. It is the amount of time in seconds that the switch waits before sending another general query.

Default disabled

Format `set mld querier query_interval 1—18000`

Mode Global Config

no set mld querier query_interval

Use this command to set the MLD Querier Query Interval time to its default value.

Format `no set mld querier query_interval`

Mode Global Config

set mld querier timer expiry

Use this command to set the MLD Querier timer expiration period. It is the time period that the switch remains in Non-Querier mode once it has discovered that there is a Multicast Querier in the network.

Default 60 seconds

Format `set mld querier timer expiry` *60—300*

Mode Global Config

no set mld querier timer expiry

Use this command to set the MLD Querier timer expiration period to its default value.

Format `no set mld querier timer expiry`

Mode Global Config

set mld querier election participate

Use this command to enable the Snooping Querier to participate in the Querier Election process when it discovers the presence of another Querier in the VLAN. When this mode is enabled, if the Snooping Querier finds that the other Querier's source address is better (less) than the Snooping Querier's address, it stops sending periodic queries. If the Snooping Querier wins the election, then it will continue sending periodic queries.

Default disabled

Format `set mld querier election participate`

Mode VLAN Config

no set mld querier election participate

Use this command to set the snooping querier not to participate in querier election but go into a non-querier mode as soon as it discovers the presence of another querier in the same VLAN.

Format `no set mld querier election participate`

Mode VLAN Config

show mldsnooping querier

Use this command to display MLD Snooping Querier information. Configured information is displayed whether or not MLD Snooping Querier is enabled.

Format `show mldsnooping querier [{detail | vlan` *vlanid*`}]`

Mode Privileged EXEC

When the optional arguments *vlanid* are not used, the command displays the following information.

Field	*Description*
Admin Mode	Indicates whether or not MLD Snooping Querier is active on the switch.
Admin Version	Indicates the version of MLD that will be used while sending out the queries. This is defaulted to `MLD v1` and it cannot be changed.
Querier Address	Shows the IP address which will be used in the IPv6 header while sending out MLD queries. It can be configured using the appropriate command.
Query Interval	Shows the amount of time in seconds that a Snooping Querier waits before sending out the periodic general query.
Querier Timeout	Displays the amount of time to wait in the Non-Querier operational state before moving to a Querier state.

When you specify a value for *vlanid*, the following information appears.

Field	*Description*
VLAN Admin Mode	Indicates whether MLD Snooping Querier is active on the VLAN.
VLAN Operational State	Indicates whether MLD Snooping Querier is in Querier" or Non-Querier" state. When the switch is in Querier state, it will send out periodic general queries. When in Non-Querier state, it will wait for moving to Querier state and does not send out any queries.
VLAN Operational Max Response Time	Indicates the time to wait before removing a Leave from a host upon receiving a Leave request. This value is calculated dynamically from the Queries received from the network. If the Snooping Switch is in Querier state, then it is equal to the configured value.
Querier Election Participate	Indicates whether the MLD Snooping Querier participates in querier election if it discovers the presence of a querier in the VLAN.
Querier VLAN Address	The IP address will be used in the IPv6 header while sending out MLD queries on this VLAN. It can be configured using the appropriate command.
Operational Version	This version of IPv6 will be used while sending out MLD queriers on this VLAN.
Last Querier Address	Indicates the IP address of the most recent Querier from which a Query was received.
Last Querier Version	Indicates the MLD version of the most recent Querier from which a Query was received on this VLAN.

When the optional argument `detail` is used, the command shows the global information and the information for all Querier-enabled VLANs.

Port Security Commands

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

Note: To enable the SNMP trap specific to port security, see "snmp-server enable traps violation" on page 87.

port-security

This command enables port locking on an interface, a range of interfaces, or at the system level.

Default disabled

Format `port-security`

Mode
- Global Config (to enable port locking globally)
- Interface Config (to enable port locking on an interface or range of interfaces)

no port-security

This command disables port locking for one (Interface Config) or all (Global Config) ports.

Format `no port-security`

Mode
- Global Config
- Interface Config

port-security max-dynamic

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

Default 600

Format `port-security max-dynamic` *`maxvalue`*

Mode Interface Config

no port-security max-dynamic

This command resets the maximum number of dynamically locked MAC addresses allowed on a specific port to its default value.

Format `no port-security max-dynamic`

Mode Interface Config

port-security max-static

This command sets the maximum number of statically locked MAC addresses allowed on a port.

Default 20

Format `port-security max-static` *`maxvalue`*

Mode Interface Config

no port-security max-static

This command sets maximum number of statically locked MAC addresses to the default value.

Format `no port-security max-static`

Mode Interface Config

port-security mac-address

This command adds a MAC address to the list of statically locked MAC addresses for an interface or range of interfaces. The *`vid`* is the VLAN ID.

Format `port-security mac-address` *`mac-address vid`*

Mode Interface Config

no port-security mac-address

This command removes a MAC address from the list of statically locked MAC addresses.

Format `no port-security mac-address` *`mac-address vid`*

Mode Interface Config

port-security mac-address move

This command converts dynamically locked MAC addresses to statically locked addresses for an interface or range of interfaces.

Format `port-security mac-address move`

Mode Interface Config

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

Term	*Definition*
Admin Mode	Port Locking mode for the entire system. This field displays if you do not supply any parameters.

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

Term	*Definition*
Admin Mode	Port Locking mode for the Interface.
Dynamic Limit	Maximum dynamically allocated MAC Addresses.
Static Limit	Maximum statically allocated MAC Addresses.
Violation Trap Mode	Whether violation traps are enabled.

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

Term	*Definition*
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

Term	*Definition*
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

Term	*Definition*
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 on an interface or a range of interfaces.

Default disabled

Format `lldp transmit`

Mode Interface Config

no lldp transmit

Use this command to return the local data transmission capability to the default.

Format `no lldp transmit`

Mode Interface Config

lldp receive

Use this command to enable the LLDP receive capability on an interface or a range of interfaces.

Default disabled

Format `lldp receive`

Mode Interface Config

no lldp receive

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

Format `no lldp receive`

Mode Interface Config

lldp timers

Use this command to set the timing parameters for local data transmission on ports enabled for LLDP. The *interval-seconds* determines the number of seconds to wait between transmitting local data LLDPDUs. The range is 1–32768 seconds. The *hold-value* is the multiplier on the transmit interval that sets the TTL in local data LLDPDUs. The multiplier range is 2–10. The *reinit-seconds* is the delay before 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 from an interface or range of interfaces. Use *sys-name* to transmit the system name TLV. To configure the system name, see "snmp-server" on page 84. 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 214.

Default no optional TLVs are included

Format `lldp transmit-tlv [sys-desc] [sys-name] [sys-cap] [port-desc]`

Mode Interface Config

no lldp transmit-tlv

Use this command to remove an optional TLV from the LLDPDUs. Use the command without parameters to remove all optional TLVs from the LLDPDU.

Format `no lldp transmit-tlv [sys-desc] [sys-name] [sys-cap] [port-desc]`

Mode Interface Config

lldp transmit-mgmt

Use this command to include transmission of the local system management address information in the LLDPDUs. This command ca be used to configure a single interface or a range of interfaces.

Format `lldp transmit-mgmt`

Mode Interface Config

no lldp transmit-mgmt

Use this command to include transmission of the local system management address information in the LLDPDUs. Use this command to cancel inclusion of the management information in LLDPDUs.

Format `no lldp transmit-mgmt`

Mode Interface Config

lldp notification

Use this command to enable remote data change notifications on an interface or a range of interfaces.

Default disabled

Format `lldp notification`

Mode Interface Config

no lldp notification

Use this command to disable notifications.

Default disabled

Format `no lldp notification`

Mode Interface Config

lldp notification-interval

Use this command to configure how frequently the system sends remote data change notifications. The *`interval`* parameter is the number of seconds to wait between sending notifications. The valid interval range is 5–3600 seconds.

Default 5

Format `lldp notification-interval` *`interval`*

Mode Global Config

no lldp notification-interval

Use this command to return the notification interval to the default value.

Format `no lldp notification-interval`

Mode Global Config

clear lldp statistics

Use this command to reset all LLDP statistics, including MED-related information.

Format `clear lldp statistics`

Mode Privileged Exec

clear lldp remote-data

Use this command to delete all information from the LLDP remote data table, including MED-related information.

Format `clear lldp remote-data`

Mode Global Config

show lldp

Use this command to display a summary of the current LLDP configuration.

Format `show lldp`

Mode Privileged Exec

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

show lldp interface

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

Format `show lldp interface {slot/port | all}`

Mode Privileged Exec

Term	*Definition*
Interface	The interface in a slot/port format.
Link	Shows whether the link is up or down.
Transmit	Shows whether the interface transmits LLDPDUs.
Receive	Shows whether the interface receives LLDPDUs.
Notify	Shows whether the interface sends remote data change notifications.

Term	*Definition*
TLVs	Shows whether the interface sends optional TLVs in the LLDPDUs. The TLV codes can be 0 (Port Description), 1 (System Name), 2 (System Description), or 3 (System Capability).
Mgmt	Shows whether the interface transmits system management address information in the LLDPDUs.

show lldp statistics

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

Format `show lldp statistics {slot/port | all}`

Mode Privileged Exec

Term	*Definition*
Last Update	The amount of time since the last update to the remote table in days, hours, minutes, and seconds.
Total Inserts	Total number of inserts to the remote data table.
Total Deletes	Total number of deletes from the remote data table.
Total Drops	Total number of times the complete remote data received was not inserted due to insufficient resources.
Total Ageouts	Total number of times a complete remote data entry was deleted because the Time to Live interval expired.

The table contains the following column headings:

Term	*Definition*
Interface	The interface in slot/port format.
Transmit Total	Total number of LLDP packets transmitted on the port.
Receive Total	Total number of LLDP packets received on the port.
Discards	Total number of LLDP frames discarded on the port for any reason.
Errors	The number of invalid LLDP frames received on the port.
Ageouts	Total number of times a complete remote data entry was deleted for the port because the Time to Live interval expired.
TVL Discards	The number of TLVs discarded.
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

Term	*Definition*
Local Interface	The interface that received the LLDPDU from the remote device.
RemID	An internal identifier to the switch to mark each remote device to the system.
Chassis ID	The ID that is sent by a remote device as part of the LLDP message, it is usually a MAC address of the device.
Port ID	The port number that transmitted the LLDPDU.
System Name	The system name of the remote device.

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

```
(Switching) #show lldp remote-device all

LLDP Remote Device Summary

Local
Interface RemID    Chassis ID            Port ID             System Name
-------  -------   --------------------  ------------------  ------------------
0/1
0/2
0/3
0/4
0/5
0/6
0/7        2       00:FC:E3:90:01:0F     00:FC:E3:90:01:11
0/7        3       00:FC:E3:90:01:0F     00:FC:E3:90:01:12
0/7        4       00:FC:E3:90:01:0F     00:FC:E3:90:01:13
0/7        5       00:FC:E3:90:01:0F     00:FC:E3:90:01:14
0/7        1       00:FC:E3:90:01:0F     00:FC:E3:90:03:11
0/7        6       00:FC:E3:90:01:0F     00:FC:E3:90:04:11
0/8
0/9
0/10
0/11
0/12
--More-- or (q)uit
```

show lldp remote-device detail

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

Format `show lldp remote-device detail slot/port`

Mode Privileged EXEC

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

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

```
(Switching) #show lldp remote-device detail 0/7

LLDP Remote Device Detail

Local Interface: 0/7

Remote Identifier: 2
Chassis ID Subtype: MAC Address
Chassis ID: 00:FC:E3:90:01:0F
Port ID Subtype: MAC Address
Port ID: 00:FC:E3:90:01:11
System Name:
System Description:
Port Description:
System Capabilities Supported:
System Capabilities Enabled:
Time to Live: 24 seconds
```

show lldp local-device

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

Format `show lldp local-device {slot/port | all}`

Mode Privileged EXEC

Term	*Definition*
Interface	The interface in a slot/port format.
Port ID	The port ID associated with this interface.
Port Description	The port description associated with the interface.

show lldp local-device detail

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

Format `show lldp local-device detail slot/port`

Mode Privileged EXEC

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

LLDP-MED Commands

Link Layer Discovery Protocol - Media Endpoint Discovery (LLDP-MED) (ANSI-TIA-1057) provides an extension to the LLDP standard. Specifically, LLDP-MED provides extensions for network configuration and policy, device location, Power over Ethernet (PoE) management and inventory management.

lldp med

Use this command to enable MED on an interface or a range of interfaces. By enabling MED, you will be effectively enabling the transmit and receive function of LLDP.

Default disabled

Format `lldp med`

Mode Interface Config

no lldp med

Use this command to disable MED.

Format `no lldp med`

Mode Interface Config

lldp med confignotification

Use this command to configure an interface or a range of interfaces to send the topology change notification.

Default disabled

Format `lldp med confignotification`

Mode Interface Config

no ldp med confignotification

Use this command to disable notifications.

Format `no lldp med confignotification`

Mode Interface Config

lldp med transmit-tlv

Use this command to specify which optional Type Length Values (TLVs) in the LLDP MED set will be transmitted in the Link Layer Discovery Protocol Data Units (LLDPDUs) from this interface or a range of interfaces.

Default By default, the capabilities and network policy TLVs are included.

Format `lldp med transmit-tlv [capabilities] [ex-pd] [ex-pse] [inventory] [location] [network-policy]`

Mode Interface Config

Term	*Definition*
capabilities	Transmit the LLDP capabilities TLV.
ex-pd	Transmit the LLDP extended PD TLV.
ex-pse	Transmit the LLDP extended PSE TLV.
inventory	Transmit the LLDP inventory TLV.
location	Transmit the LLDP location TLV.
network-policy	Transmit the LLDP network policy TLV.

no lldp med transmit-tlv

Use this command to remove a TLV.

Format `no lldp med transmit-tlv [capabilities] [network-policy] [ex-pse] [ex-pd] [location] [inventory]`

Mode Interface Config

lldp med all

Use this command to configure LLDP-MED on all the ports.

Format `lldp med all`

Mode Global Config

lldp med confignotification all

Use this command to configure all the ports to send the topology change notification.

Format `lldp med confignotification all`

Mode Global Config

lldp med faststartrepeatcount

Use this command to set the value of the fast start repeat count. `[count]` is the number of LLDP PDUs that will be transmitted when the product is enabled. The range is 1 to 10.

Default 3

Format `lldp med faststartrepeatcount [count]`

Mode Global Config

no lldp med faststartrepeatcount

Use this command to return to the factory default value.

Format `no lldp med faststartrepeatcount`

Mode Global Config

lldp med transmit-tlv all

Use this command to specify which optional Type Length Values (TLVs) in the LLDP MED set will be transmitted in the Link Layer Discovery Protocol Data Units (LLDPDUs).

Default By default, the capabilities and network policy TLVs are included.

Format `lldp med transmit-tlv all [capabilities] [ex-pd] [ex-pse] [inventory] [location] [network-policy]`

Mode Global Config

Term	*Definition*
capabilities	Transmit the LLDP capabilities TLV.
ex-pd	Transmit the LLDP extended PD TLV.
ex-pse	Transmit the LLDP extended PSE TLV.
inventory	Transmit the LLDP inventory TLV.
location	Transmit the LLDP location TLV.
network-policy	Transmit the LLDP network policy TLV.

no lldp med transmit-tlv

Use this command to remove a TLV.

Format `no lldp med transmit-tlv [capabilities] [network-policy] [ex-pse] [ex-pd] [location] [inventory]`

Mode Global Config

show lldp med

Use this command to display a summary of the current LLDP MED configuration.

Format `show lldp med`

Mode Privileged Exec

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

```
(Routing) #show lldp med
LLDP MED Global Configuration

Fast Start Repeat Count: 3
Device Class: Network Connectivity

(Routing) #
```

show lldp med interface

Use this command to display a summary of the current LLDP MED configuration for a specific interface. The variable slot/port indicates a specific physical interface. The keyword `all` indicates all valid LLDP interfaces.

Format `show lldp med interface {`*`unit/slot/port`* `| all}`

Mode Privileged Exec

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

```
(Routing) #show lldp med interface all

Interface  Link    configMED operMED   ConfigNotify TLVsTx
---------  ------  --------- --------  ------------ -----------
1/0/1      Down    Disabled  Disabled  Disabled     0,1
1/0/2      Up      Disabled  Disabled  Disabled     0,1
1/0/3      Down    Disabled  Disabled  Disabled     0,1
1/0/4      Down    Disabled  Disabled  Disabled     0,1
1/0/5      Down    Disabled  Disabled  Disabled     0,1
1/0/6      Down    Disabled  Disabled  Disabled     0,1
1/0/7      Down    Disabled  Disabled  Disabled     0,1
1/0/8      Down    Disabled  Disabled  Disabled     0,1
1/0/9      Down    Disabled  Disabled  Disabled     0,1
1/0/10     Down    Disabled  Disabled  Disabled     0,1
1/0/11     Down    Disabled  Disabled  Disabled     0,1
1/0/12     Down    Disabled  Disabled  Disabled     0,1
1/0/13     Down    Disabled  Disabled  Disabled     0,1
1/0/14     Down    Disabled  Disabled  Disabled     0,1

TLV Codes: 0- Capabilities,       1- Network Policy
           2- Location,           3- Extended PSE
           4- Extended Pd,        5- Inventory
--More-- or (q)uit
(Routing) #show lldp med interface 1/0/2

Interface  Link    configMED operMED   ConfigNotify TLVsTx
---------  ------  --------- --------  ------------ -----------
1/0/2      Up      Disabled  Disabled  Disabled     0,1
```

```
TLV Codes: 0- Capabilities,       1- Network Policy
           2- Location,           3- Extended PSE
           4- Extended Pd,        5- Inventory

(Routing) #
```

show lldp med local-device detail

Use this command to display detailed information about the LLDP MED data that a specific interface transmits. slot/port indicates a specific physical interface.

Format `show lldp med local-device detail slot/port`

Mode Privileged EXEC

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

```
(Routing) #show lldp med local-device detail 1/0/8

LLDP MED Local Device Detail

Interface: 1/0/8

Network Policies
Media Policy Application Type : voice
Vlan ID: 10
Priority: 5
DSCP: 1
Unknown: False
Tagged: True

Media Policy Application Type : streamingvideo
Vlan ID: 20
Priority: 1
DSCP: 2
Unknown: False
Tagged: True

Inventory
Hardware Rev: xxx xxx xxx
Firmware Rev: xxx xxx xxx
Software Rev: xxx xxx xxx
Serial Num: xxx xxx xxx
Mfg Name: xxx xxx xxx
Model Name: xxx xxx xxx
Asset ID: xxx xxx xxx

Location
Subtype: elin
Info: xxx xxx xxx

Extended POE
Device Type: pseDevice

Extended POE PSE
```

```
Available: 0.3 Watts
Source: primary
Priority: critical

Extended POE PD

Required: 0.2 Watts
Source: local
Priority: low
```

show lldp med remote-device

Use this command to display the summary information about remote devices that transmit current LLDP MED data to the system. You can show information about LLDP MED remote data received on all valid LLDP interfaces or on a specific physical interface.

Format `show lldp med remote-device {slot/port | all}`

Mode Privileged EXEC

Term	*Definition*
Local Interface	The interface that received the LLDPDU from the remote device.
Remote ID	An internal identifier to the switch to mark each remote device to the system.
Device Class	Device classification of the remote device.

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

```
(Routing) #show lldp med remote-device all

LLDP MED Remote Device Summary

Local
Interface  Remote ID  Device Class
---------  ---------  ------------
1/0/8          1          Class I
1/0/9          2          Not Defined
1/0/10         3          Class II
1/0/11         4          Class III
1/0/12         5          Network Con
```

show lldp med remote-device detail

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

Format `show lldp med remote-device detail slot/port`

Mode Privileged EXEC

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

```
(Routing) #show lldp med remote-device detail 1/0/8
```

```
LLDP MED Remote Device Detail

Local Interface: 1/0/8
Remote Identifier: 18
Capabilities
MED Capabilities Supported: capabilities, networkpolicy, location, extendedpse
MED Capabilities Enabled: capabilities, networkpolicy
Device Class: Endpoint Class I

Network Policies
Media Policy Application Type : voice
Vlan ID: 10
Priority: 5
DSCP: 1
Unknown: False
Tagged: True

Media Policy Application Type : streamingvideo
Vlan ID: 20
Priority: 1
DSCP: 2
Unknown: False
Tagged: True


Inventory
Hardware Rev: xxx xxx xxx
Firmware Rev: xxx xxx xxx
Software Rev: xxx xxx xxx
Serial Num: xxx xxx xxx
Mfg Name: xxx xxx xxx
Model Name: xxx xxx xxx
Asset ID: xxx xxx xxx

Location
Subtype: elin
Info: xxx xxx xxx

Extended POE
Device Type: pseDevice

Extended POE PSE
Available: 0.3 Watts
Source: primary
Priority: critical

Extended POE PD

Required: 0.2 Watts
Source: local
Priority: low
```

Denial of Service Commands

This section describes the commands you use to configure Denial of Service (DoS) Control. DWS-4000 software provides support for classifying and blocking specific types of Denial of Service attacks. You can configure your system to monitor and block these types of attacks:

- **SIP = DIP:** Source IP address = Destination IP address.
- **First Fragment:**TCP Header size smaller then configured value.
- **TCP Fragment:** IP Fragment Offset = 1.
- **TCP Flag:** TCP Flag SYN set and Source Port < 1024 or TCP Control Flags = 0 and TCP Sequence Number = 0 or TCP Flags FIN, URG, and PSH set and TCP Sequence Number = 0 or TCP Flags SYN and FIN set.
- **L4 Port:** Source TCP/UDP Port = Destination TCP/UDP Port.
- **ICMP:** Limiting the size of ICMP Ping packets.

Note: Monitoring and blocking of the types of attacks listed below are only supported on the BCM56224, BCM56514, BCM56624, BCM56634, BCM56636 and BCM56820platforms.

- **SMAC = DMAC:** Source MAC address = Destination MAC address.
- TCP Port: Source TCP Port = Destination TCP Port.
- UDP Port: Source UDP Port = Destination UDP Port.
- **TCP Flag & Sequence:** TCP Flag SYN set and Source Port < 1024 or TCP Control Flags = 0 and TCP Sequence Number = 0 or TCP Flags FIN, URG, and PSH set and TCP Sequence Number = 0 or TCP Flags SYN and FIN set.
- **TCP Offset:** TCP Header Offset = 1.
- **TCP SYN:** TCP Flag SYN set.
- **TCP SYN & FIN:** TCP Flags SYN and FIN set.
- **TCP FIN & URG & PSH:** TCP Flags FIN and URG and PSH set and TCP Sequence Number = 0.
- **ICMP V6**: Limiting the size of ICMPv6 Ping packets.
- **ICMP Fragment**: Checks for fragmented ICMP packets.

dos-control all

This command enables Denial of Service protection checks globally.

Default	disabled
Format	`dos-control all`
Mode	Global Config

no dos-control all

This command disables Denial of Service prevention checks globally.

Format `no dos-control all`

Mode Global Config

dos-control sipdip

This command enables Source IP address = Destination IP address (SIP = DIP) Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress with SIP = DIP, the packets will be dropped if the mode is enabled.

Default disabled

Format `dos-control sipdip`

Mode Global Config

no dos-control sipdip

This command disables Source IP address = Destination IP address (SIP = DIP) Denial of Service prevention.

Format `no dos-control sipdip`

Mode Global Config

dos-control firstfrag

This command enables Minimum TCP Header Size Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having a TCP Header Size smaller then the configured value, the packets will be dropped if the mode is enabled.The default is *disabled*. If you enable dos-control firstfrag, but do not provide a Minimum TCP Header Size, the system sets that value to 20.

Default disabled (20)

Format `dos-control firstfrag [`*0*–*255*`]`

Mode Global Config

no dos-control firstfrag

This command sets Minimum TCP Header Size Denial of Service protection to the default value of *disabled*.

Format `no dos-control firstfrag`

Mode Global Config

dos-control tcpfrag

This command enables TCP Fragment Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. 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 dos-control tcpfrag`

Mode Global Config

dos-control tcpflag

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

Default disabled

Format `dos-control tcpflag`

Mode Global Config

no dos-control tcpflag

This command sets disables TCP Flag Denial of Service protections.

Format `no dos-control tcpflag`

Mode Global Config

dos-control l4port

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

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

Default disabled

Format `dos-control l4port`

Mode Global Config

no dos-control l4port

This command disables L4 Port Denial of Service protections.

Format `no dos-control l4port`

Mode Global Config

dos-control 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

dos-control smacdmac

This command enables Source MAC address = Destination MAC address (SMAC = DMAC) Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress with SMAC = DMAC, the packets will be dropped if the mode is enabled.

Default disabled

Format `dos-control smacdmac`

Mode Global Config

no dos-control smacdmac

This command disables Source MAC address = Destination MAC address (SMAC = DMAC) DoS protection.

Format `no dos-control smacdmac`

Mode Global Config

dos-control tcpport

This command enables TCP L4 source = destination port number (Source TCP Port = Destination TCP Port) Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress with Source TCP Port = Destination TCP Port, the packets will be dropped if the mode is enabled.

Default disabled

Format `dos-control tcpport`

Mode Global Config

no dos-control tcpport

This command disables TCP L4 source = destination port number (Source TCP Port = Destination TCP Port) Denial of Service protection.

Format `no dos-control smacdmac`

Mode Global Config

dos-control udpport

This command enables UDP L4 source = destination port number (Source UDP Port = Destination UDP Port) DoS protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress with Source UDP Port = Destination UDP Port, the packets will be dropped if the mode is enabled.

Default disabled

Format `dos-control udpport`

Mode Global Config

no dos-control udpport

This command disables UDP L4 source = destination port number (Source UDP Port = Destination UDP Port) Denial of Service protection.

Format `no dos-control udpport`

Mode Global Config

dos-control tcpflagseq

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

Default disabled

Format `dos-control tcpflagseq`

Mode Global Config

no dos-control tcpflagseq

This command sets disables TCP Flag and Sequence Denial of Service protection.

Format `no dos-control tcpflagseq`

Mode Global Config

dos-control tcpoffset

This command enables TCP Offset Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having TCP Header Offset equal to one (1), the packets will be dropped if the mode is enabled.

Default disabled

Format `dos-control tcpoffset`

Mode Global Config

no dos-control tcpoffset

This command disabled TCP Offset Denial of Service protection.

Format `no dos-control tcpoffset`

Mode Global Config

dos-control tcpsyn

This command enables TCP SYN and L4 source = 0–1023 Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having TCP flag SYN set and an L4 source port from 0 to 1023, the packets will be dropped if the mode is enabled.

Default disabled

Format `dos-control tcpsyn`

Mode Global Config

no dos-control tcpsyn

This command sets disables TCP SYN and L4 source = 0–1023 Denial of Service protection.

Format `no dos-control tcpsyn`

Mode Global Config

dos-control tcpsynfin

This command enables TCP SYN and FIN Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having TCP flags SYN and FIN set, the packets will be dropped if the mode is enabled.

Default disabled

Format `dos-control tcpsynfin`

Mode Global Config

no dos-control tcpsynfin

This command sets disables TCP SYN & FIN Denial of Service protection.

Format `no dos-control tcpsynfin`

Mode Global Config

dos-control tcpfinurgpsh

This command enables TCP FIN and URG and PSH and SEQ = 0 checking Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having TCP FIN, URG, and PSH all set and TCP Sequence Number set to 0, the packets will be dropped if the mode is enabled.

Default disabled

Format `dos-control tcpfinurgpsh`

Mode Global Config

no dos-control tcpfinurgpsh

This command sets disables TCP FIN and URG and PSH and SEQ = 0 checking Denial of Service protections.

Format `no dos-control tcpfinurgpsh`

Mode Global Config

dos-control icmpv4

This command enables Maximum ICMPv4 Packet Size Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attack. If ICMPv4 Echo Request (PING) packets ingress having a size greater than the configured value, the packets will be dropped if the mode is enabled.

Default disabled (512)

Format `dos-control icmpv4 0–16384`

Mode Global Config

no dos-control icmpv4

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

Format `no dos-control icmpv4`

Mode Global Config

dos-control icmpv6

This command enables Maximum ICMPv6 Packet Size Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attack. If ICMPv6 Echo Request (PING) packets ingress having a size greater than the configured value, the packets will be dropped if the mode is enabled.

Default disabled (512)

Format `dos-control icmpv6 0–16384`

Mode Global Config

no dos-control icmpv6

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

Format `no dos-control icmpv6`

Mode Global Config

dos-control icmpfrag

This command enables ICMP Fragment Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having fragmented ICMP packets, the packets will be dropped if the mode is enabled.

Default disabled

Format `dos-control icmpfrag`

Mode Global Config

no dos-control icmpfrag

This command disabled ICMP Fragment Denial of Service protection.

Format `no dos-control icmpfrag`

Mode Global Config

show dos-control

This command displays Denial of Service configuration information.

Format `show dos-control`

Mode Privileged EXEC

Term	*Definition*
First Fragment Mode	May be enabled or disabled. The factory default is disabled.
Min TCP Hdr Size <0–255>	The factory default is 20.
ICMP Mode	May be enabled or disabled. The factory default is disabled.
Max ICMPv4 Pkt Size	The range is 0–1023. The factory default is 512.
Max ICMPv6 Pkt Size	The range is 0–16384. The factory default is 512.
ICMP Fragment Mode	May be enabled or disabled. The factory default is disabled.
L4 Port Mode	May be enabled or disabled. The factory default is disabled.
TCP Port Mode	May be enabled or disabled. The factory default is disabled.
UDP Port Mode	May be enabled or disabled. The factory default is disabled.
SIPDIP Mode	May be enabled or disabled. The factory default is disabled.
SMACDMAC Mode	May be enabled or disabled. The factory default is disabled.
TCP Flag Mode	May be enabled or disabled. The factory default is disabled.
TCP FIN&URG& PSH Mode	May be enabled or disabled. The factory default is disabled.
TCP Flag & Sequence Mode	May be enabled or disabled. The factory default is disabled.
TCP SYN Mode	May be enabled or disabled. The factory default is disabled.
TCP SYN & FIN Mode	May be enabled or disabled. The factory default is disabled.

Term	*Definition*
TCP Fragment Mode	May be enabled or disabled. The factory default is disabled.
TCP Offset Mode	May be enabled or disabled. The factory default is disabled.

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

Term	*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

Term	*Definition*
VLAN ID	The VLAN in which the MAC address is learned.
MAC Address	A multicast MAC address for which the switch has forwarding or filtering information. The format is 6 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB.
Type	The type of the entry. 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

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

ISDP Commands

This section describes the commands you use to configure the industry standard Discovery Protocol (ISDP). ISDP is a proprietary Layer 2 network protocol which inter-operates with Cisco network equipment and is used to share information between neighboring devices (routers, bridges, access servers, and switches).

Through the operation of ISDP the device discovers information about its neighbors such as:

- Device identifier
- Port ID
- Remote device model (Device ID + Software version + Platform + Capabilities)

isdp run

This command enables ISDP on the switch.

Default Enabled

Format `isdp run`

Mode Global Config

no isdp run

This command disables ISDP on the switch.

Format `no isdp run`

Mode Global Config

isdp holdtime

This command configures the hold time for ISDP packets that the switch transmits. The hold time specifies how long a receiving device should store information sent in the ISDP packet before discarding it. The range is given in seconds.

Default 180 seconds

Format `isdp holdtime` *`10—255`*

Mode Global Config

isdp timer

This command sets the period of time between sending new ISDP packets. The range is given in seconds.

Default 30 seconds

Format `isdp timer` *`5—254`*

Mode Global Config

isdp advertise-v2

This command enables the sending of ISDP version 2 packets from the device.

Default Enabled

Format `isdp advertise-v2`

Mode Global Config

no isdp advertise-v2

This command disables the sending of ISDP version 2 packets from the device.

Format `no isdp advertise-v2`

Mode Global Config

isdp enable

This command enables ISDP on an interface or range of interfaces.

Note: ISDP must be enabled both globally and on the interface in order for the interface to transmit ISDP packets. If ISDP is globally disabled on the switch, the interface will not transmit ISDP packets, regardless of the ISDP status on the interface. To enable ISDP globally, use the command "isdp run" on page 393.

Default Enabled

Format `isdp enable`

Mode Interface Config

no isdp enable

This command disables ISDP on the interface.

Format `no isdp enable`

Mode Interface Config

clear isdp counters

This command clears ISDP counters.

Format `clear isdp counters`

Mode Privileged EXEC

clear isdp table

This command clears entries in the ISDP table.

Format `clear isdp table`

Mode Privileged EXEC

show isdp

This command displays global ISDP settings.

Format `show isdp`

Mode Privileged EXEC

Term	*Definition*
Timer	The frequency with which this device sends ISDP packets. This value is given in seconds.
Hold Time	The length of time the receiving device should save information sent by this device. This value is given in seconds.
ISDPv2 Advertisements	The setting for sending ISDPv2 packets. If disabled, version 1 packets are transmitted.
Device ID	The Device ID advertised by this device. The format of this Device ID is characterized by the value of the Device ID Format object.
Device ID Format Capability	Indicates the Device ID format capability of the device. • `serialNumber` indicates that the device uses a serial number as the format for its Device ID. • `macAddress` indicates that the device uses a Layer 2 MAC address as the format for its Device ID. • `other` indicates that the device uses its platform-specific format as the format for its Device ID.

Term	*Definition*
Device ID Format	Indicates the Device ID format of the device. • `serialNumber` indicates that the value is in the form of an ASCII string containing the device serial number. • `macAddress` indicates that the value is in the form of a Layer 2 MAC address. • `other` indicates that the value is in the form of a platform specific ASCII string containing info that identifies the device. For example, ASCII string contains serialNumber appended/prepended with system name.

show isdp interface

This command displays ISDP settings for the specified interface.

Format `show isdp interface {all | slot/port}`

Mode Privileged EXEC

Term	*Definition*
Mode	ISDP mode enabled/disabled status for the interface(s).

show isdp entry

This command displays ISDP entries. If the device id is specified, then only entries for that device are shown.

Format `show isdp entry {all | deviceid}`

Mode Privileged EXEC

Term	*Definition*
Device ID	The device ID associated with the neighbor which advertised the information.
IP Addresses	The IP address(es) associated with the neighbor.
Platform	The hardware platform advertised by the neighbor.
Interface	The interface (slot/port) on which the neighbor's advertisement was received.
Port ID	The port ID of the interface from which the neighbor sent the advertisement.
Hold Time	The hold time advertised by the neighbor.
Version	The software version that the neighbor is running.
Advertisement Version	The version of the advertisement packet received from the neighbor.
Capability	ISDP Functional Capabilities advertised by the neighbor.

show isdp neighbors

This command displays the list of neighboring devices.

Format `show isdp neighbors [{slot/port | detail}]`

Mode Privileged EXEC

Term	*Definition*
Device ID	The device ID associated with the neighbor which advertised the information.
IP Addresses	The IP addresses associated with the neighbor.
Capability	ISDP functional capabilities advertised by the neighbor.
Platform	The hardware platform advertised by the neighbor.
Interface	The interface (slot/port) on which the neighbor's advertisement was received.
Port ID	The port ID of the interface from which the neighbor sent the advertisement.
Hold Time	The hold time advertised by the neighbor.
Advertisement Version	The version of the advertisement packet received from the neighbor.
Entry Last Changed Time	Displays when the entry was last modified.
Version	The software version that the neighbor is running.

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

```
(Switching) #show isdp neighbors detail

Device ID                       0001f45f1bc0
Address(es):
    IP Address:                 10.27.7.57
Capability                      Router Trans Bridge Switch IGMP
Platform                        SecureStack C2
Interface                       0/48
Port ID                         ge.3.14
Holdtime                        131
Advertisement Version           2
Entry last changed time         0 days 00:01:59
Version:                        05.00.56
```

show isdp traffic

This command displays ISDP statistics.

Format show isdp traffic

Mode Privileged EXEC

Term	*Definition*
ISDP Packets Received	Total number of ISDP packets received
ISDP Packets Transmitted	Total number of ISDP packets transmitted
ISDPv1 Packets Received	Total number of ISDPv1 packets received
ISDPv1 Packets Transmitted	Total number of ISDPv1 packets transmitted
ISDPv2 Packets Received	Total number of ISDPv2 packets received
ISDPv2 Packets Transmitted	Total number of ISDPv2 packets transmitted
ISDP Bad Header	Number of packets received with a bad header
ISDP Checksum Error	Number of packets received with a checksum error
ISDP Transmission Failure	Number of packets which failed to transmit
ISDP Invalid Format	Number of invalid packets received
ISDP Table Full	Number of times a neighbor entry was not added to the table due to a full database
ISDP IP Address Table Full	Displays the number of times a neighbor entry was added to the table without an IP address.

debug isdp packet

This command enables tracing of ISDP packets processed by the switch. ISDP must be enabled on both the device and the interface in order to monitor packets for a particular interface.

Format `debug isdp packet [{receive | transmit}]`

Mode Privileged EXEC

no debug isdp packet

This command disables tracing of ISDP packets on the receive or the transmit sides or on both sides.

Format `no debug isdp packet [{receive | transmit}]`

Mode Privileged EXEC

Section 6: Routing Commands

This chapter describes the routing commands available in the DWS-4000 CLI. The Routing Commands chapter contains the following sections:

Note: The commands in this section are in one of three functional groups:

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

Address Resolution Protocol Commands

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

arp

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

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

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. The parameter *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 or range of interfaces. Without proxy ARP, a device only responds to an ARP request if the target IP address is an address configured on the interface where the ARP request arrived. With proxy ARP, the device may also respond if the target IP address is reachable. The device only responds if all next hops in its route to the destination are through interfaces other than the interface that received the ARP request.

Default enabled

Format `ip proxy-arp`

Mode Interface Config

no ip proxy-arp

This command disables proxy ARP on a router interface.

Format `no ip proxy-arp`

Mode Interface Config

arp cachesize

This command configures the ARP cache size. The ARP cache size value is a platform specific integer value. The default size also varies depending on the platform.

Format `arp cachesize` *`platform specific integer value`*

Mode Global Config

no arp cachesize

This command configures the default ARP cache size.

Format `no arp cachesize`

Mode Global Config

arp dynamicrenew

This command enables the ARP component to automatically renew dynamic ARP entries when they age out. When an ARP entry reaches its maximum age, the system must decide whether to retain or delete the entry. If the entry has recently been used to forward data packets, the system will renew the entry by sending an ARP request to the neighbor. If the neighbor responds, the age of the ARP cache entry is reset to 0 without removing the entry from the hardware. Traffic to the host continues to be forwarded in hardware without interruption. If the entry is not being used to forward data packets, then the entry is deleted from the ARP cache, unless the dynamic renew option is enabled. If the dynamic renew option is enabled, the system sends an ARP request to renew the entry. When an entry is not renewed, it is removed from the hardware and subsequent data packets to the host trigger an ARP request. Traffic to the host may be lost until the router receives an ARP reply from the host. Gateway entries, entries for a neighbor router, are always renewed. The dynamic renew option applies only to host entries.

The disadvantage of enabling dynamic renew is that once an ARP cache entry is created, that cache entry continues to take space in the ARP cache as long as the neighbor continues to respond to ARP requests, even if no traffic is being forwarded to the neighbor. In a network where the number of potential neighbors is greater than the ARP cache capacity, enabling dynamic renew could prevent some neighbors from communicating because the ARP cache is full.

Default disabled

Format `arp dynamicrenew`

Mode Privileged EXEC

no arp dynamicrenew

This command prevents dynamic ARP entries from renewing when they age out.

Format `no arp dynamicrenew`

Mode Privileged EXEC

arp purge

This command causes the specified IP address to be removed from the ARP cache. Only entries of type dynamic or gateway are affected by this command.

Format `arp purge 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

clear arp-switch

Use this command to clear the contents of the switch's Address Resolution Protocol (ARP) table that contains entries learned through the Management port. To observe whether this command is successful, `ping` from the remote system to the DUT. Issue the `show arp switch` command to see the ARP entries. Then issue the `clear arp-switch` command and check the `show arp switch` entries. There will be no more arp entries.

Format `clear arp-switch`

Mode Privileged EXEC

show arp

This command displays the Address Resolution Protocol (ARP) cache. The displayed results are not the total ARP entries. To view the total ARP entries, the operator should view the `show arp` results in conjunction with the `show arp switch` results.

Format `show arp`

Mode Privileged EXEC

Term	*Definition*
Age Time (seconds)	The time it takes for an ARP entry to age out. This is configurable. Age time is measured in seconds.
Response Time (seconds)	The time it takes for an ARP request timeout. This value is configurable. Response time is measured in seconds.
Retries	The maximum number of times an ARP request is retried. This value is configurable.
Cache Size	The maximum number of entries in the ARP table. This value is configurable.
Dynamic Renew Mode	Displays whether the ARP component automatically attempts to renew dynamic ARP entries when they age out.
Total Entry Count Current / Peak	The total entries in the ARP table and the peak entry count in the ARP table.
Static Entry Count Current / Max	The static entry count in the ARP table and maximum static entry count in the ARP table.

The following are displayed for each ARP entry:

Term	*Definition*
IP Address	The IP address of a device on a subnet attached to an existing routing interface.
MAC Address	The hardware MAC address of that device.
Interface	The routing slot/port associated with the device ARP entry.
Type	The type that is configurable. The possible values are Local, Gateway, Dynamic and Static.
Age	The current age of the ARP entry since last refresh (in hh:mm:ss format)

show arp brief

This command displays the brief Address Resolution Protocol (ARP) table information.

Format `show arp brief`

Mode Privileged EXEC

Term	*Definition*
Age Time (seconds)	The time it takes for an ARP entry to age out. This value is configurable. Age time is measured in seconds.
Response Time (seconds)	The time it takes for an ARP request timeout. This value is configurable. Response time is measured in seconds.

Term	*Definition*
Retries	The maximum number of times an ARP request is retried. This value is configurable.
Cache Size	The maximum number of entries in the ARP table. This value is configurable.
Dynamic Renew Mode	Displays whether the ARP component automatically attempts to renew dynamic ARP entries when they age out.
Total Entry Count Current / Peak	The total entries in the ARP table and the peak entry count in the ARP table.
Static Entry Count Current / Max	The static entry count in the ARP table and maximum static entry count in the ARP table.

show arp switch

This command displays the contents of the switch's Address Resolution Protocol (ARP) table.

Format `show arp switch`

Mode Privileged EXEC

Term	*Definition*
IP Address	The IP address of a device on a subnet attached to the switch.
MAC Address	The hardware MAC address of that device.
Interface	The routing 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 or range of interfaces. You can view the current value for this function with the `show ip brief` command. The value is labeled as *Routing Mode*.

Default disabled

Format `routing`

Mode Interface Config

no routing

This command disables routing for an interface.

You can view the current value for this function with the `show ip brief` command. The value is labeled as *Routing Mode*.

Format `no routing`

Mode Interface Config

ip routing

This command enables the IP Router Admin Mode for the master switch.

Format `ip routing`

Mode Global Config

no ip routing

This command disables the IP Router Admin Mode for the master switch.

Format `no ip routing`

Mode Global Config

ip address

This command configures an IP address on an interface or range of interfaces. You can also use this command to configure one or more secondary IP addresses on the interface.The 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 adds 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 in a.b.c.d format where the range for a, b, c, and d is 1–255. The value for *subnetmask* is a 4-digit dotted-decimal number which represents the Subnet Mask of the interface. To remove all of the IP addresses (primary and secondary) configured on the interface, enter the command `no ip address`.

Format `no ip address [{`*ipaddr subnetmask* `[secondary]}]`

Mode Interface Config

ip address dhcp

This command enables the DHCPv4 client on an in-band interface so that it can acquire network information, such as the IP address, subnet mask, and default gateway, from a network DHCP server. When DHCP is enabled on the interface, the system automatically deletes all manually configured IPv4 addresses on the interface.

Default disabled

Format `ip address dhcp`

Mode Interface Config

no ip address dhcp

This command releases a leased address and disables DHCPv4 on an interface.

Format `no ip address dhcp`

Mode Interface Config

ip default-gateway

This command manually configures a default gateway for the switch. Only one default gateway can be configured. If you invoke this command multiple times, each command replaces the previous value.

Format `ip default-gateway` *`ipaddr`*

Mode Global Config

no ip default-gateway

This command removes the default gateway address from the configuration.

Format `no ip default-gateway` *`ipaddr`*

Mode Interface Config

release dhcp

Use this command to force the DHCPv4 client to release the leased address from the specified interface.

Format `release dhcp slot/port`

Mode Privileged EXEC

renew dhcp

Use this command to force the DHCPv4 client to immediately renew an IPv4 address lease on the specified interface.

Note: This command can be used on in-band ports as well as the service or network (out-of-band) port.

Format `renew dhcp slot/port`

Mode Privileged EXEC

ip route

This command configures a static route. The *ipaddr* parameter is a valid IP address, and *subnetmask* is a valid subnet mask. The *nexthopip* parameter is a valid IP address of the next hop router. Specifying Null0 as nexthop parameter adds a static reject route. The optional *preference* parameter is an integer (value from 1 to 255) that allows you to specify the preference value (sometimes called *administrative distance*) of an individual static route. Among routes to the same destination, the route with the lowest preference value is the route entered into the forwarding database. By specifying the preference of a static route, you control whether a static route is more or less preferred than routes from dynamic routing protocols. The preference also controls whether a static route is more or less preferred than other static routes to the same destination. A route with a preference of 255 cannot be used to forward traffic.

For the static routes to be visible, you must perform the following steps:

- Enable ip routing globally.
- Enable ip routing for the interface.
- Confirm that the associated link is also up.

Default preference—1

Format `ip route ipaddr subnetmask [nexthopip | Null0] [preference]`

Mode Global Config

no ip route

This command deletes a single next hop to a destination static route. If you use the *nexthopip* parameter, the next hop is deleted. If you use the *preference* value, the preference value of the static route is reset to its default.

Format `no ip route ipaddr subnetmask [{nexthopip [preference] | Null0}]`

Mode Global Config

ip route default

This command configures the default route. The value for *nexthopip* is a valid IP address of the next hop router. The *preference* is an integer value from 1 to 255. A route with a preference of 255 cannot be used to forward traffic.

Default preference—1

Format `ip route default nexthopip [preference]`

Mode Global Config

no ip route default

This command deletes all configured default routes. If the optional *nexthopip* parameter is designated, the specific next hop is deleted from the configured default route and if the optional preference value is designated, the preference of the configured default route is reset to its default.

Format `no ip route default [{nexthopip | preference}]`

Mode Global Config

ip route distance

This command sets the default distance (preference) for static routes. Lower route distance values are preferred when determining the best route. The `ip route` and `ip route default` commands allow you to optionally set the distance (preference) of an individual static route. The default distance is used when no distance is specified in these commands. Changing the default distance does not update the distance of existing static routes, even if they were assigned the original default distance. The new default distance will only be applied to static routes created after invoking the `ip route distance` command.

Default 1

Format `ip route distance` *1—255*

Mode Global Config

no ip route distance

This command sets the default static route preference value in the router. Lower route preference values are preferred when determining the best route.

Format `no ip route distance`

Mode Global Config

ip netdirbcast

This command enables the forwarding of network-directed broadcasts on an interface or range of interfaces. When enabled, network directed broadcasts are forwarded. When disabled they are dropped.

Default disabled

Format `ip netdirbcast`

Mode Interface Config

no ip netdirbcast

This command disables the forwarding of network-directed broadcasts. When disabled, network directed broadcasts are dropped.

Format `no ip netdirbcast`

Mode Interface Config

ip mtu

This command sets the IP Maximum Transmission Unit (MTU) on a routing interface or range of interfaces. The IP MTU is the size of the largest IP packet that can be transmitted on the interface without fragmentation. Forwarded packets are dropped if they exceed the IP MTU of the outgoing interface.

Packets originated on the router, such as OSPF packets, may be fragmented by the IP stack.

OSPF advertises the IP MTU in the Database Description packets it sends to its neighbors during database exchange. If two OSPF neighbors advertise different IP MTUs, they will not form an adjacency. (unless OSPF has been instructed to ignore differences in IP MTU with the `ip ospf mtu-ignore` command.)

Note: The IP MTU size refers to the maximum size of the IP packet (IP Header + IP payload). It does not include any extra bytes that may be required for Layer-2 headers. To receive and process packets, the Ethernet MTU (see "mtu" on page 214) must take into account the size of the Ethernet header.

Default 1500 bytes

Format `ip mtu` *68–9198*

Mode Interface Config

no ip mtu

This command resets the ip mtu to the default value.

Format `no ip mtu`

Mode Interface Config

encapsulation

This command configures the link layer encapsulation type for the packet on an interface or range of interfaces. The encapsulation type can be `ethernet` or `snap`.

Default ethernet

Format `encapsulation {ethernet | snap}`

Mode Interface Config

Note: Routed frames are always ethernet encapsulated when a frame is routed to a VLAN.

show dhcp lease

This command displays a list of IPv4 addresses currently leased from a DHCP server on a specific in-band interface or all in-band interfaces. This command does not apply to service or network ports.

Format `show dhcp lease [interface slot/port]`

Modes Privileged EXEC

Term	*Definition*
IP address, Subnet mask	The IP address and network mask leased from the DHCP server
DHCP Lease server	The IPv4 address of the DHCP server that leased the address.
State	State of the DHCPv4 Client on this interface
DHCP transaction ID	The transaction ID of the DHCPv4 Client
Lease	The time (in seconds) that the IP address was leased by the server
Renewal	The time (in seconds) when the next DHCP renew Request is sent by DHCPv4 Client to renew the leased IP address
Rebind	The time (in seconds) when the DHCP Rebind process starts
Retry count	Number of times the DHCPv4 client sends a DHCP REQUEST message before the server responds

show ip brief

This command displays all the summary information of the IP, including the ICMP rate limit configuration and the global ICMP Redirect configuration.

Format `show ip brief`

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
Default Time to Live	The computed TTL (Time to Live) of forwarding a packet from the local router to the final destination.
Routing Mode	Shows whether the routing mode is enabled or disabled.
Maximum Next Hops	The maximum number of next hops the packet can travel.
Maximum Routes	The maximum number of routes the packet can travel.
ICMP Rate Limit Interval	Shows how often the token bucket is initialized with burst-size tokens. *Burst-interval* is from 0 to 2147483647 milliseconds. The default *burst-interval* is 1000 msec.
ICMP Rate Limit Burst Size	Shows the number of ICMPv4 error messages that can be sent during one *burst-interval*. The range is from 1 to 200 messages. The default value is 100 messages.
ICMP Echo Replies	Shows whether ICMP Echo Replies are enabled or disabled.
ICMP Redirects	Shows whether ICMP Redirects are enabled or disabled.

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

```
(Switch) #show ip brief

Default Time to Live.......................... 64
```

```
Routing Mode................................. Disabled
Maximum Next Hops............................ 4
Maximum Routes............................... 6000
ICMP Rate Limit Interval..................... 1000 msec
ICMP Rate Limit Burst Size................... 100 messages
ICMP Echo Replies............................ Enabled
ICMP Redirects............................... Enabled
```

show ip interface

This command displays all pertinent information about the IP interface.

Format `show ip interface slot/port`

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
Routing Interface Status	Determine the operational status of IPv4 routing Interface. The possible values are Up or Down.
Primary IP Address	The primary IP address and subnet masks for the interface. This value appears only if you configure it.
Method	Shows whether the IP address was configured manually or acquired from a DHCP server.
Secondary IP Address	One or more secondary IP addresses and subnet masks for the interface. This value appears only if you configure it.
Helper IP Address	The helper IP addresses configured by the command "ip helper-address (Interface Config)" on page 435.
Routing Mode	The administrative mode of router interface participation. The possible values are enable or disable. This value is configurable.
Administrative Mode	The administrative mode of the specified interface. The possible values of this field are enable or disable. This value is configurable.
Forward Net Directed Broadcasts	Displays whether forwarding of network-directed broadcasts is enabled or disabled. This value is configurable.
Proxy ARP	Displays whether Proxy ARP is enabled or disabled on the system.
Local Proxy ARP	Displays whether Local Proxy ARP is enabled or disabled on the interface.
Active State	Displays whether the interface is active or inactive. An interface is considered active if its link is up and it is in forwarding state.
Link Speed Data Rate	An integer representing the physical link data rate of the specified interface. This is measured in Megabits per second (Mbps).
MAC Address	The burned in physical address of the specified interface. The format is 6 two-digit hexadecimal numbers that are separated by colons.
Encapsulation Type	The encapsulation type for the specified interface. The types are: Ethernet or SNAP.
IP MTU	The maximum transmission unit (MTU) size of a frame, in bytes.
Bandwidth	Shows the bandwidth of the interface.

Term	*Definition*
Destination Unreachables	Displays whether ICMP Destination Unreachables may be sent (enabled or disabled).
ICMP Redirects	Displays whether ICMP Redirects may be sent (enabled or disabled).

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

```
(switch)#show ip interface 1/0/2

Routing Interface Status..................... Down
Primary IP Address........................... 1.2.3.4/255.255.255.0
Method....................................... Manual
Secondary IP Address(es)..................... 21.2.3.4/255.255.255.0
.............................................. 22.2.3.4/255.255.255.0
Helper IP Address............................ 1.2.3.4
.............................................. 1.2.3.5
Routing Mode................................. Disable
Administrative Mode.......................... Enable
Forward Net Directed Broadcasts.............. Disable
Proxy ARP.................................... Enable
Local Proxy ARP.............................. Disable
Active State................................. Inactive
Link Speed Data Rate......................... Inactive
MAC Address.................................. 00:10:18:82:0C:68
Encapsulation Type........................... Ethernet
IP MTU....................................... 1500
Bandwidth.................................... 100000 kbps
Destination Unreachables..................... Enabled
ICMP Redirects............................... Enabled
```

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

Term	*Definition*
Interface	Valid slot and port number separated by a forward slash.
State	Routing operational state of the interface.
IP Address	The IP address of the routing interface in 32-bit dotted decimal format.
IP Mask	The IP mask of the routing interface in 32-bit dotted decimal format.
Netdir Bcast	Indicates if IP forwards net-directed broadcasts on this interface. Possible values are Enable or Disable.
MultiCast Fwd	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}]`

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
Route Codes	The key for the routing protocol codes that might appear in the routing table output.

The `show ip route` command displays the routing tables in the following format:

```
Code   IP-Address/Mask [Preference/Metric] via Next-Hop, Route-Timestamp, Interface
```

The columns for the routing table display the following information:

Term	*Definition*
Code	The codes for the routing protocols that created the routes.
Default Gateway	The IP address of the default gateway. When the system does not have a more specific route to a packet's destination, it sends the packet to the default gateway.
IP-Address/Mask	The IP-Address and mask of the destination network corresponding to this route.
Preference	The administrative distance associated with this route. Routes with low values are preferred over routes with higher values.
Metric	The cost associated with this route.
via Next-Hop	The outgoing router IP address to use when forwarding traffic to the next router (if any) in the path toward the destination.
Route-Timestamp	The last updated time for dynamic routes. The format of Route-Timestamp will be • Days:Hours:Minutes if days > = 1 • Hours:Minutes:Seconds if days < 1
Interface	The outgoing router interface to use when forwarding traffic to the next destination. For reject routes, the next hop interface would be Null0 interface.

To administratively control the traffic destined to a particular network and prevent it from being forwarded through the router, you can configure a static reject route on the router. Such traffic would be discarded and the ICMP destination unreachable message is sent back to the source. This is typically used for preventing routing loops. The reject route added in the RTO is of the type **OSPF Inter-Area**. Reject routes (routes of REJECT type installed by any protocol) are not redistributed by OSPF/RIP. Reject routes are supported in both OSPFv2 and OSPFv3.

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

```
(Routing) #show ip route

Route Codes: R - RIP Derived, O - OSPF Derived, C - Connected, S - Static
       B - BGP Derived, IA - OSPF Inter Area
       E1 - OSPF External Type 1, E2 - OSPF External Type 2
       N1 - OSPF NSSA External Type 1, N2 - OSPF NSSA External Type 2

Default gateway is 1.1.1.2

C 1.1.1.0/24 [0/1] directly connected, 0/11
C 2.2.2.0/24 [0/1] directly connected, 0/1
C 5.5.5.0/24 [0/1] directly connected, 0/5
S 7.0.0.0/8 [1/0] directly connected, Null0
OIA 10.10.10.0/24 [110/6] via 5.5.5.2,   00h:00m:01s,  0/5
C 11.11.11.0/24 [0/1] directly connected,   0/11
S 12.0.0.0/8 [5/0] directly connected, Null0
S 23.0.0.0/8 [3/0] directly connected, Null0
```

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]`

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
Connected Routes	The total number of connected routes in the routing table.
Static Routes	Total number of static routes in the routing table.
RIP Routes	Total number of routes installed by RIP protocol.
BGP Routes	Total number of routes installed by BGP protocol.
OSPF Routes	Total number of routes installed by OSPF protocol.
Reject Routes	Total number of reject routes installed by all protocols.
Total Routes	Total number of routes in the routing table.

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

```
(Routing) #show ip route summary
```

```
Connected Routes.............................1
Static Routes................................7
RIP Routes...................................0
BGP Routes...................................0
OSPF Routes..................................0
  Intra Area Routes..........................0
  Inter Area Routes..........................0
  External Type-1 Routes.....................0
  External Type-2 Routes.....................0
Reject Routes................................2
Total routes.................................8
```

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

Term	*Definition*
Local	The local route preference value.
Static	The static route preference value.
OSPF Intra	The OSPF Intra route preference value.
OSPF Inter	The OSPF Inter route preference value.
OSPF External	The OSPF External route preference value.
RIP	The RIP route preference value.
BGP4	The BGP-4 route preference value.
Configured Default Gateway	The route preference value of the statically-configured default gateway
DHCP Default Gateway	The route preference value of the default gateway learned from the DHCP server.

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 or range of interfaces.

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 multicast

This command configures the destination IP address for router advertisements. If no destination IP address is configured, router advertisements are forwarded to 224.0.0.1 by default. You can also configure the IP address as 255.255.255.255 (or use the no form of the command) to instead send router advertisements to the limited broadcast address.

Format `ip irdp multicast ip address`

Mode Interface Config

no ip irdp multicast

By default, router advertisements are sent to 224.0.0.1. To instead send router advertisements to the limited broadcast address, 255.255.255.255, use the no form of this command.

Format `no ip irdp multicast`

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

Term	*Definition*
Interface	The slot/port that matches the rest of the information in the row.
Ad Mode	The advertise mode, which indicates whether router discovery is enabled or disabled on this interface.
Dest Address	The destination IP address for router advertisements.
Max Int	The maximum advertise interval, which is the maximum time, in seconds, allowed between sending router advertisements from the interface.
Min Int	The minimum advertise interval, which is the minimum time, in seconds, allowed between sending router advertisements from the interface.
Hold Time	The amount of time, in seconds, that a system should keep the router advertisement before discarding it.
Preference	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 enables routing on a VLAN. The *vlanid* value has a range from 1 to 4093. The *[interface ID]* value has a range from 1 to 128. Typically, you will not supply the interface ID argument, and the system automatically selects the interface ID. However, if you specify an interface ID, the interface ID becomes the port number in the slot/port for the VLAN routing interface. If you select an interface ID that is already in use, the CLI displays an error message and does not create the VLAN interface. For products that use text-based configuration, including the interface ID in the vlan routing command for the text configuration ensures that the slot/port for the VLAN interface stays the same across a restart. Keeping the slot/port the same ensures that the correct interface configuration is applied to each interface when the system restarts.

Format `vlan routing vlanid [interface ID]`

Mode VLAN Config

no vlan routing

This command deletes routing on a VLAN.

Format `no vlan routing vlanid`

Mode VLAN Config

Example: Example 1 shows the command specifying a vlanid value. The interface ID argument is not used.

```
(Switch)(Vlan)#vlan 14
(Switch)(Vlan)#vlan routing 14 ?
<cr>                    Press enter to execute the command.
<1-128>                 Enter interface ID
```

Typically, you press <**Enter**> without supplying the Interface ID value; the system automatically selects the interface ID.

Example: In Example 2, the command specifies interface ID 51 for VLAN 14 interface. The interface ID becomes the port number in the slot/port for the VLAN routing interface. In this example, slot/port is 4/51 for VLAN 14 interface.

```
(Switch)(Vlan)#vlan 14 51
(Switch)(Vlan)#
(Switch)#show ip vlan
MAC Address used by Routing VLANs:   00:11:88:59:47:36

           Logical
VLAN ID   Interface        IP Address       Subnet Mask
-------  -------------  ---------------  ---------------
10       4/1            172.16.10.1      255.255.255.0
11       4/50           172.16.11.1      255.255.255.0
```

```
12       4/3             172.16.12.1      255.255.255.0
13       4/4             172.16.13.1      255.255.255.0
14       4/51            0.0.0.0          0.0.0.0  <--u/s/p is 4/51 for VLAN 14 interface
```

Example: In Example 3, you select an interface ID that is already in use. In this case, the CLI displays an error message and does not create the VLAN interface.

```
(Switch) #show ip vlan

MAC Address used by Routing VLANs:   00:11:88:59:47:36

           Logical
VLAN ID   Interface        IP Address       Subnet Mask
-------  -------------  ---------------  ---------------
10       4/1             172.16.10.1      255.255.255.0
11       4/50            172.16.11.1      255.255.255.0
12       4/3             172.16.12.1      255.255.255.0
13       4/4             172.16.13.1      255.255.255.0
14       4/51            0.0.0.0          0.0.0.0

(Switch)#config

(Switch)(Config)#exit

(Switch)#vlan database

(Switch)(Vlan)#vlan 15

(Switch)(Vlan)#vlan routing 15 1

Interface ID 1 is already assigned to another interface
```

Example: The show running configuration command always lists the interface ID for each routing VLAN, as shown in Example 4 below.

```
(Switch) #show running-config
!Current Configuration:
!
!System Description "Alpha HELIX 56314 Development System - 48 GB, 4.24.10.4, VxWorks 6.5"
!System Software Version "4.24.10.4"
!System Up Time          "0 days 0 hrs 22 mins 19 secs"
!Additional Packages     None
!Current SNTP Synchronized Time: Not Synchronized
!
set prompt "02.08"
network protocol dhcp
vlan database
vlan 10-14
vlan routing 10 1
vlan routing 12 3
vlan routing 13 4
vlan routing 11 50
vlan routing 14 51
```

show ip vlan

This command displays the VLAN routing information for all VLANs with routing enabled.

Format `show ip vlan`

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
MAC Address used by Routing VLANs	The MAC Address associated with the internal bridge-router interface (IBRI). The same MAC Address is used by all VLAN routing interfaces. It will be displayed above the per-VLAN information.
VLAN ID	The identifier of the VLAN.
Logical Interface	The logical slot/port associated with the VLAN routing interface.
IP Address	The IP address associated with this VLAN.
Subnet Mask	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 (Global Config)

Use this command in Global Config mode to enable the administrative mode of VRRP on the router.

Default none

Format `ip vrrp`

Mode Global Config

no ip vrrp

Use this command in Global Config mode to disable the default administrative mode of VRRP on the router.

Format `no ip vrrp`

Mode Global Config

ip vrrp (Interface Config)

Use this command in Interface Config mode to create a virtual router associated with the interface or range of interfaces. The parameter *vrid* is the virtual router ID, which has an integer value range from 1 to 255.

Format `ip vrrp vrid`

Mode Interface Config

no ip vrrp

Use this command in Interface Config mode to delete the virtual router associated with the interface. The virtual Router ID, *vrid*, is an integer value that ranges from 1 to 255.

Format `no ip vrrp vrid`

Mode 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 IP address value for an interface or range of interfaces. 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

no ip vrrp ip

Use this command in Interface Config mode to delete a secondary IP address value from the interface. To delete the primary IP address, you must delete the virtual router on the interface.

Format `no ip vrrp vrid ipaddress secondary`

Mode Interface Config

ip vrrp accept-mode

Use this command to allow the VRRP Master to accept ping packets sent to one of the virtual router's IP addresses.

Note: VRRP accept-mode allows only ICMP Echo Request packets. No other type of packet is allowed to be delivered to a VRRP address.

Default disabled

Format `ip vrrp vrid accept-mode`

Mode Interface Config

no ip vrrp accept-mode

Use this command to prevent the VRRP Master from accepting ping packets sent to one of the virtual router's IP addresses.

Format `no ip vrrp vrid accept-mode`

Mode Interface Config

ip vrrp authentication

This command sets the authorization details value for the virtual router configured on a specified interface or range of interfaces. 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 or range of interfaces.

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 or range of interfaces. 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 or range of interfaces.

Format `no ip vrrp vrid preempt`

Mode • Interface Config

ip vrrp priority

This command sets the priority of a router within a VRRP group. It can be used to configure an interface or a range of interfaces. Higher values equal higher priority. The range is from 1 to 254. The parameter *vrid* is the virtual router ID, whose range is from 1 to 255.

The router with the highest priority is elected master. If a router is configured with the address used as the address of the virtual router, the router is called the *address owner*. The priority of the address owner is always 255 so that the address owner is always master. If the master has a priority less than 255 (it is not the address owner) and you configure the priority of another router in the group higher than the master's priority, the router will take over as master only if preempt mode is enabled.

Default 100 unless the router is the address owner, in which case its priority is automatically set to 255.

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 or range of interfaces.

Format `no ip vrrp vrid priority`

Mode Interface Config

ip vrrp timers advertise

This command sets the frequency, in seconds, that an interface or range of interfaces 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 or range of interfaces.

Format `no ip vrrp vrid timers advertise`

Mode Interface Config

ip vrrp track interface

Use this command to alter the priority of the VRRP router based on the availability of its interfaces. This command is useful for tracking interfaces that are not configured for VRRP. Only IP interfaces are tracked. A tracked interface is up if the IP on that interface is up. Otherwise, the tracked interface is down. You can use this command to configure a single interface or a range of interfaces.

When the tracked interface is down or the interface has been removed from the router, the priority of the VRRP router will be decremented by the value specified in the *priority* argument. When the interface is up for IP protocol, the priority will be incremented by the *priority* value.

A VRRP configured interface can track more than one interface. When a tracked interface goes down, then the priority of the router will be decreased by 10 (the default priority decrement) for each downed interface. The default priority decrement is changed using the *priority* argument. The default priority of the virtual router is 100, and the default decrement priority is 10. By default, no interfaces are tracked. If you specify just the interface to be tracked, without giving the optional priority, then the default priority will be set. The default priority decrement is 10.

Default priority: 10

Format `ip vrrp vrid track interface slot/port [decrement priority]`

Mode Interface Config

no ip vrrp track interface

Use this command to remove the interface or range of interfaces from the tracked list or to restore the priority decrement to its default.

Format `no ip vrrp vrid track interface slot/port [decrement]`

Mode Interface Config

ip vrrp track ip route

Use this command to track the route reachability on an interface or range of interfaces. When the tracked route is deleted, the priority of the VRRP router will be decremented by the value specified in the *priority* argument. When the tracked route is added, the priority will be incremented by the same.

A VRRP configured interface can track more than one route. When a tracked route goes down, then the priority of the router will be decreased by 10 (the default priority decrement) for each downed route. By default no routes are tracked. If you specify just the route to be tracked, without giving the optional priority, then the default priority will be set. The default priority decrement is 10. The default priority decrement is changed using the *priority* argument.

Default priority: 10

Format `ip vrrp vrid track ip route ip-address/prefix-length [decrement priority]`

Mode Interface Config

no ip vrrp track ip route

Use this command to remove the route from the tracked list or to restore the priority decrement to its default. When removing a tracked IP route from the tracked list, the priority should be incremented by the decrement value if the route is not reachable.

Format `no ip vrrp vrid track interface slot/port [decrement]`

Mode Interface Config

show ip vrrp interface stats

This command displays the statistical information about each virtual router configured on the switch.

Format `show ip vrrp interface stats slot/port vrid`

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
Uptime	The time that the virtual router has been up, in days, hours, minutes and seconds.
Protocol	The protocol configured on the interface.
State Transitioned to Master	The total number of times virtual router state has changed to MASTER.
Advertisement Received	The total number of VRRP advertisements received by this virtual router.
Advertisement Interval Errors	The total number of VRRP advertisements received for which advertisement interval is different than the configured value for this virtual router.

Term	*Definition*
Authentication Failure	The total number of VRRP packets received that don't pass the authentication check.
IP TTL errors	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	The total number of VRRP packets received by virtual router with a priority of '0'.
Zero Priority Packets Sent	The total number of VRRP packets sent by the virtual router with a priority of '0'.
Invalid Type Packets Received	The total number of VRRP packets received by the virtual router with invalid 'type' field.
Address List Errors	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	The total number of VRRP packets received with unknown authentication type.
Authentication Type Mismatch	The total number of VRRP advertisements received for which 'auth type' not equal to locally configured one for this virtual router.
Packet Length Errors	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 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

Term	*Definition*
VRRP Admin Mode	The administrative mode for VRRP functionality on the switch.
Router Checksum Errors	The total number of VRRP packets received with an invalid VRRP checksum value.
Router Version Errors	The total number of VRRP packets received with Unknown or unsupported version number.
Router VRID Errors	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. Use the output of the command to verify the track interface and track IP route configurations.

Format `show ip vrrp interface slot/port` *`vrid`*

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
IP Address	The configured IP address for the Virtual router.
VMAC address	The VMAC address of the specified router.
Authentication type	The authentication type for the specific virtual router.
Priority	The priority value for the specific virtual router, taking into account any priority decrements for tracked interfaces or routes.
Configured Priority	The priority configured through the `ip vrrp` *`vrid`* `priority 1–254` command.
Advertisement interval	The advertisement interval in seconds for the specific virtual router.
Pre-Empt Mode	The preemption mode configured on the specified virtual router.
Administrative Mode	The status (Enable or Disable) of the specific router.
Accept Mode	When enabled, the VRRP Master can accept ping packets sent to one of the virtual router's IP addresses.
State	The state (Master/backup) of the virtual router.

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

```
show ip vrrp interface <u/s/p> vrid

Primary IP Address.............................. 1.1.1.5
VMAC Address.................................... 00:00:5e:00:01:01
Authentication Type............................. None
Priority........................................ 80
  Configured priority........................... 100
Advertisement Interval (secs)................... 1
Pre-empt Mode................................... Enable
Administrative Mode............................. Enable
Accept Mode..................................... Enable
State........................................... Initialized
Track Interface          State          DecrementPriority
---------------         ------          -----------------

<1/0/1>                  down               10
TrackRoute  (pfx/len)        State         DecrementPriority
-----------------------   ------         -----------------
10.10.10.1/255.255.255.0    down              10
```

show ip vrrp interface brief

This command displays information about each virtual router configured on the switch. This command takes no options. It displays information about each virtual router.

Format `show ip vrrp interface brief`

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
Interface	*slot/port*
VRID	The router ID of the virtual router.
IP Address	The virtual router IP address.
Mode	Indicates whether the virtual router is enabled or disabled.
State	The state (Master/backup) of the virtual router.

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 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

show bootpdhcprelay

This command displays the BootP/DHCP Relay information.

Format `show bootpdhcprelay`

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
Maximum Hop Count	The maximum allowable relay agent hops.
Minimum Wait Time (Seconds)	The minimum wait time.
Admin Mode	Indicates whether relaying of requests is enabled or disabled.
Server IP Address	The IP address for the BootP/DHCP Relay server.
Circuit Id Option Mode	The DHCP circuit Id option which may be enabled or disabled.
Requests Received	The number or requests received.
Requests Relayed	The number of requests relayed.
Packets Discarded	The number of packets discarded.

IP Helper Commands

This section describes the commands to configure and monitor the IP Helper agent. IP Helper relays DHCP and other broadcast UDP packets from a local client to one or more servers which are not on the same network at the client.

The IP Helper feature provides a mechanism that allows a router to forward certain configured UDP broadcast packets to a particular IP address. This allows various applications to reach servers on non-local subnets, even if the application was designed to assume a server is always on a local subnet and uses broadcast packets (with either the limited broadcast address 255.255.255.255, or a network directed broadcast address) to reach the server.

The network administrator can configure relay entries both globally and on routing interfaces. Each relay entry maps an ingress interface and destination UDP port number to a single IPv4 address (the helper address). The network administrator may configure multiple relay entries for the same interface and UDP port, in which case the relay agent relays matching packets to each server address. Interface configuration takes priority over global configuration. That is, if a packet's destination UDP port matches any entry on the ingress interface, the packet is handled according to the interface configuration. If the packet does not match any entry on the ingress interface, the packet is handled according to the global IP helper configuration.

The network administrator can configure discard relay entries, which direct the system to discard matching packets. Discard entries are used to discard packets received on a specific interface when those packets would otherwise be relayed according to a global relay entry. Discard relay entries may be configured on interfaces, but are not configured globally.

In addition to configuring the server addresses, the network administrator also configures which UDP ports are forwarded. Certain UDP port numbers can be specified by name in the UI as a convenience, but the network administrator can configure a relay entry with any UDP port number. The network administrator may configure relay entries that do not specify a destination UDP port. The relay agent relays assumes these entries match packets with the UDP destination ports listed in Table 10. This is the list of default ports.

Table 10: Default Ports - UDP Port Numbers Implied by Wildcard

Protocol	*UDP Port Number*
IEN-116 Name Service	42
DNS	53
NetBIOS Name Server	137
NetBIOS Datagram Server	138
TACACS Server	49
Time Service	37
DHCP	67
Trivial File Transfer Protocol (TFTP)	69

The system limits the number of relay entries to four times the maximum number of routing interfaces. The network administrator can allocate the relay entries as he likes. There is no limit to the number of relay entries on an individual interface, and no limit to the number of servers for a given {interface, UDP port} pair.

The relay agent relays DHCP packets in both directions. It relays broadcast packets from the client to one or more DHCP servers, and relays to the client packets that the DHCP server unicasts back to the relay agent. For other protocols, the relay agent only relays broadcast packets from the client to the server. Packets from the server back to the client are assumed to be unicast directly to the client. Because there is no relay in the return direction for protocols other than DHCP, the relay agent retains the source IP address from the original client packet. The relay agent uses a local IP address as the source IP address of relayed DHCP client packets.

When a switch receives a broadcast UDP packet on a routing interface, the relay agent checks if the interface is configured to relay the destination UDP port. If so, the relay agent unicasts the packet to the configured server IP addresses. Otherwise, the relay agent checks if there is a global configuration for the destination UDP port. If so, the relay agent unicasts the packet to the configured server IP addresses. Otherwise the packet is not relayed. Note that if the packet matches a discard relay entry on the ingress interface, then the packet is not forwarded, regardless of the global configuration.

The relay agent only relays packets that meet the following conditions:

- The destination MAC address must be the all-ones broadcast address (FF:FF:FF:FF:FF:FF)
- The destination IP address must be the limited broadcast address (255.255.255.255) or a directed broadcast address for the receive interface.
- The IP time-to-live (TTL) must be greater than 1.
- The protocol field in the IP header must be UDP (17).
- The destination UDP port must match a configured relay entry.

clear ip helper statistics

Use this command to reset to zero the statistics displayed in the `show ip helper statistics` command.

Format `clear ip helper statistics`

Mode Privileged EXEC

Example: The following shows an example of the command.

```
(switch) #clear ip helper statistics
```

ip helper-address (Global Config)

Use this command to configure the relay of certain UDP broadcast packets received on any interface. This command can be invoked multiple times, either to specify multiple server addresses for a given UDP port number or to specify multiple UDP port numbers handled by a specific server.

Default `No helper addresses are configured.`

Format `ip helper-address server-address [dest-udp-port | dhcp | domain | isakmp | mobile-ip | nameserver | netbios-dgm | netbios-ns | ntp | pim-auto-rp | rip | tacacs | tftp | time]`

Mode Global Config

Parameter	*Description*
server-address	The IPv4 unicast or directed broadcast address to which relayed UDP broadcast packets are sent. The server address cannot be an IP address configured on any interface of the local router.
dest-udp-port	A destination UDP port number from 0 to 65535.
port-name	The destination UDP port may be optionally specified by its name. Whether a port is specified by its number or its name has no effect on behavior. The names recognized are as follows: • dhcp (port 67) • domain (port 53) • isakmp (port 500) • mobile-ip (port 434) • nameserver (port 42) • netbios-dgm (port 138) • netbios-ns (port 137) • ntp (port 123) • pim-auto-rp (port 496) • rip (port 520) • tacacs (port 49) • tftp (port 69) • time (port 37) Other ports must be specified by number.

Example: To relay DHCP packets received on any interface to two DHCP servers, 10.1.1.1 and 10.1.2.1, use the following commands:

```
(switch)#config
(switch)(config)#ip helper-address 10.1.1.1 dhcp
(switch)(config)#ip helper-address 10.1.2.1 dhcp
```

Example: To relay UDP packets received on any interface for all default ports to the server at 20.1.1.1, use the following commands:

```
(switch)#config
(switch)(config)#ip helper-address 20.1.1.1
```

no ip helper-address (Global Config)

Use the `no` form of the command to delete an IP helper entry. The command `no ip helper-address` with no arguments clears all global IP helper addresses.

Format `no ip helper-address [server-address [dest-udp-port | dhcp | domain | isakmp | mobile-ip | nameserver | netbios-dgm | netbios-ns | ntp | pim-auto-rp | rip | tacacs | tftp | time]`

Mode Global Config

ip helper-address (Interface Config)

Use this command to configure the relay of certain UDP broadcast packets received on a specific interface or range of interfaces. This command can be invoked multiple times on a routing interface, either to specify multiple server addresses for a given port number or to specify multiple port numbers handled by a specific server.

Default `No helper addresses are configured.`

Format `ip helper-address {server-address | discard} [dest-udp-port | dhcp | domain | isakmp | mobile ip | nameserver | netbios-dgm | netbios-ns | ntp | pim-auto-rp | rip | tacacs | tftp | time]`

Mode Interface Config

Parameter	*Description*
server-address	The IPv4 unicast or directed broadcast address to which relayed UDP broadcast packets are sent. The server address cannot be in a subnet on the interface where the relay entry is configured, and cannot be an IP address configured on any interface of the local router.
discard	Matching packets should be discarded rather than relayed, even if a global ip helper-address configuration matches the packet.
dest-udp-port	A destination UDP port number from 0 to 65535.

Parameter	*Description*
port-name	The destination UDP port may be optionally specified by its name. Whether a port is specified by its number or its name has no effect on behavior. The names recognized are as follows: • dhcp (port 67) • domain (port 53) • isakmp (port 500) • mobile-ip (port 434) • nameserver (port 42) • netbios-dgm (port 138) • netbios-ns (port 137) • ntp (port 123) • pim-auto-rp (port 496) • rip (port 520) • tacacs (port 49) • tftp (port 69) • time (port 37) Other ports must be specified by number.

Example: To relay DHCP packets received on interface 1/0/2 to two DHCP servers, 192.168.10.1 and 192.168.20.1, use the following commands:

```
(switch)#config
(switch)(config)#interface 1/0/2
(switch)(interface 1/0/2)#ip helper-address 192.168.10.1 dhcp
(switch)(interface 1/0/2)#ip helper-address 192.168.20.1 dhcp
```

Example: To relay both DHCP and DNS packets to 192.168.30.1, use the following commands:

```
(switch)#config
(switch)(config)#interface 1/0/2
(switch)(interface 1/0/2)#ip helper-address 192.168.30.1 dhcp
(switch)(interface 1/0/2)#ip helper-address 192.168.30.1 dns
```

Example: This command takes precedence over an ip helper-address command given in global configuration mode. With the following configuration, the relay agent relays DHCP packets received on any interface other than 1/0/2 and 1/0/17 to 192.168.40.1, relays DHCP and DNS packets received on 1/0/2 to 192.168.40.2, relays SNMP traps (port 162) received on interface 1/0/17 to 192.168.23.1, and drops DHCP packets received on 1/0/17:

```
(switch)#config
(switch)(config)#ip helper-address 192.168.40.1 dhcp
(switch)(config)#interface 1/0/2
(switch)(interface 1/0/2)#ip helper-address 192.168.40.2 dhcp
(switch)(interface 1/0/2)#ip helper-address 192.168.40.2 domain
(switch)(interface 1/0/2)#exit
(switch)(config)#interface 1/0/17
(switch)(interface 1/0/17)#ip helper-address 192.168.23.1 162
(switch)(interface 1/0/17)#ip helper-address discard dhcp
```

no ip helper-address (Interface Config)

Use this command to delete a relay entry on an interface. The no command with no arguments clears all helper addresses on the interface.

Format `no ip helper-address [server-address | discard ][dest-udp-port | dhcp | domain | isakmp | mobile ip | nameserver | netbios-dgm | netbios-ns | ntp | pim-auto-rp | rip | tacacs | tftp | time]`

Mode Interface Config

ip helper enable

Use this command to enable relay of UDP packets. This command can be used to temporarily disable IP helper without deleting all IP helper addresses. This command replaces the `bootpdhcprelay enable` command, but affects not only relay of DHCP packets, but also relay of any other protocols for which an IP helper address has been configured.

Default `disabled`

Format `ip helper enable`

Mode Global Config

Example: The following shows an example of the command.

```
(switch)(config)#ip helper enable
```

no ip helper enable

Use the no form of this command to disable relay of all UDP packets.

Format `no ip helper enable`

Mode Global Config

show ip helper-address

Use this command to display the IP helper address configuration.

Format `show ip helper-address [slot/port]`

Mode Privileged EXEC

Parameter	*Description*
interface	The relay configuration is applied to packets that arrive on this interface. This field is set to any for global IP helper entries.
UDP Port	The relay configuration is applied to packets whose destination UDP port is this port. Entries whose UDP port is identified as any are applied to packets with the destination UDP ports listed in Table 4.

Parameter	*Description*
Discard	If Yes, packets arriving on the given interface with the given destination UDP port are discarded rather than relayed. Discard entries are used to override global IP helper address entries which otherwise might apply to a packet.
Hit Count	The number of times the IP helper entry has been used to relay or discard a packet.
Server Address	The IPv4 address of the server to which packets are relayed.

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

```
(switch) #show ip helper-address

IP helper is enabled

    Interface   UDP Port     Discard   Hit Count   Server Address
---------------  -----------  --------  ----------  ---------------
       1/0/1             dhcp        No          10       10.100.1.254
                                                          10.100.2.254
       1/0/17             any       Yes           2
           any           dhcp        No           0       10.200.1.254
```

show ip helper statistics

Use this command to display the number of DHCP and other UDP packets processed and relayed by the UDP relay agent.

Format `show ip helper statistics`

Mode Privileged EXEC

Parameter	*Description*
DHCP client messages received	The number of valid messages received from a DHCP client. The count is only incremented if IP helper is enabled globally, the ingress routing interface is up, and the packet passes a number of validity checks, such as having a TTL>1 and having valid source and destination IP addresses.
DHCP client messages relayed	The number of DHCP client messages relayed to a server. If a message is relayed to multiple servers, the count is incremented once for each server.
DHCP server messages received	The number of DHCP responses received from the DHCP server. This count only includes messages that the DHCP server unicasts to the relay agent for relay to the client.
DHCP server messages relayed	The number of DHCP server messages relayed to a client.
UDP clients messages received	The number of valid UDP packets received. This count includes DHCP messages and all other protocols relayed. Conditions are similar to those for the first statistic in this table.
UDP clients messages relayed	The number of UDP packets relayed. This count includes DHCP messages relayed as well as all other protocols. The count is incremented for each server to which a packet is sent.

Parameter	*Description*
DHCP message hop count exceeded max	The number of DHCP client messages received whose hop count is larger than the maximum allowed. The maximum hop count is a configurable value listed in show bootpdhcprelay. A log message is written for each such failure. The DHCP relay agent does not relay these packets.
DHCP message with secs field below min	The number of DHCP client messages received whose secs field is less than the minimum value. The minimum secs value is a configurable value and is displayed in show bootpdhcprelay. A log message is written for each such failure. The DHCP relay agent does not relay these packets.
DHCP message with giaddr set to local address	The number of DHCP client messages received whose gateway address, giaddr, is already set to an IP address configured on one of the relay agent's own IP addresses. In this case, another device is attempting to spoof the relay agent's address. The relay agent does not relay such packets. A log message gives details for each occurrence.
Packets with expired TTL	The number of packets received with TTL of 0 or 1 that might otherwise have been relayed.
Packets that matched a discard entry	The number of packets ignored by the relay agent because they match a discard relay entry.

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

```
(switch)#show ip helper statistics

DHCP client messages received..................... 8
DHCP client messages relayed...................... 2
DHCP server messages received..................... 2
DHCP server messages relayed...................... 2
UDP client messages received...................... 8
UDP client messages relayed....................... 2
DHCP message hop count exceeded max............... 0
DHCP message with secs field below min......... 0
DHCP message with giaddr set to local address.. 0
Packets with expired TTL.......................... 0
Packets that matched a discard entry........... 0
```

Open Shortest Path First Commands

This section describes the commands you use to view and configure Open Shortest Path First (OSPF), which is a link-state routing protocol that you use to route traffic within a network. This section contains the following subsections:

General OSPF Commands

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

network area (OSPF)

Use this command to enable OSPFv2 on an interface and set its area ID if the IP address of an interface is covered by this network command.

Default disabled

Format `network ip-address wildcard-mask area area-id`

Mode Router OSPF Config

no network area (OSPF)

Use this command to disable the OSPFv2 on a interface if the IP address of an interface was earlier covered by this network command.

Format `no network ip-address wildcard-mask area area-id`

Mode Router OSPF 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

no area nssa default-info-originate (OSPF)

This command disables the default route advertised into the NSSA.

Format `no 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

no area nssa no-redistribute (OSPF)

This command disables the NSSA ABR so that learned external routes are redistributed to the NSSA.

Format `no 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

no area nssa no-summary (OSPF)

This command disables nssa from the summary LSAs.

Format `no 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

no area nssa translator-role (OSPF)

This command disables the nssa translator role from the specified area id.

Format `no 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

no area nssa translator-stab-intv (OSPF)

This command disables the nssa translator's *stabilityinterval* from the specified area id.

Format `no 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 16 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

auto-cost (OSPF)

By default, OSPF computes the link cost of each interface from the interface bandwidth. Faster links have lower metrics, making them more attractive in route selection. The configuration parameters in the `auto-cost reference bandwidth` and `bandwidth` commands give you control over the default link cost. You can configure for OSPF an interface bandwidth that is independent of the actual link speed. A second configuration parameter allows you to control the ratio of interface bandwidth to link cost. The link cost is computed as the ratio of a reference bandwidth to the interface bandwidth (ref_bw ÷ interface bandwidth), where interface bandwidth is defined by the `bandwidth` command. Because the default reference bandwidth is 100 Mbps, OSPF uses the same default link cost for all interfaces whose bandwidth is 100 Mbps or greater. Use the `auto-cost` command to change the reference bandwidth, specifying the reference bandwidth in megabits per second (Mbps). The reference bandwidth range is 1–4294967 Mbps.

Default 100 Mbps

Format `auto-cost reference-bandwidth 1–4294967`

Mode Router OSPF Config

no auto-cost reference-bandwidth (OSPF)

Use this command to set the reference bandwidth to the default value.

Format `no auto-cost reference-bandwidth`

Mode Router OSPF Config

capability opaque

Use this command to enable Opaque Capability on the Router. The information contained in Opaque LSAs may be used directly by OSPF or indirectly by an application wishing to distribute information throughout the OSPF domain. DWS-4000 supports the storing and flooding of Opaque LSAs of different scopes. The default value of `enabled` means that OSPF will forward opaque LSAs by default. If you want to upgrade from a previous release, where the default was disabled, opaque LSA forwarding will be enabled. If you want to disable opaque LSA forwarding, then you should enter the command no capability opaque in OSPF router configuration mode after the software upgrade.

Default enabled

Format `capability opaque`

Mode Router Config

no capability opaque

Use this command to disable opaque capability on the router.

Format `no capability opaque`

Mode Router Config

clear ip ospf

Use this command to disable and re-enable OSPF.

Format `clear ip ospf`

Mode Privileged EXEC

clear ip ospf configuration

Use this command to reset the OSPF configuration to factory defaults.

Format `clear ip ospf configuration`

Mode Privileged EXEC

clear ip ospf counters

Use this command to reset global and interface statistics.

Format `clear ip ospf counters`

Mode Privileged EXEC

clear ip ospf neighbor

Use this command to drop the adjacency with all OSPF neighbors. On each neighbor's interface, send a one-way hello. Adjacencies may then be re-established. To drop all adjacencies with a specific router ID, specify the neighbor's Router ID using the optional parameter [*neighbor-id*].

Format `clear ip ospf neighbor` *`[neighbor-id]`*

Mode Privileged EXEC

clear ip ospf neighbor interface

To drop adjacency with all neighbors on a specific interface, use the optional parameter slot/port. To drop adjacency with a specific router ID on a specific interface, use the optional parameter [*neighbor-id*].

Format `clear ip ospf neighbor interface [slot/port] [neighbor-id]`

Mode Privileged EXEC

clear ip ospf redistribution

Use this command to flush all self-originated external LSAs. Reapply the redistribution configuration and re-originate prefixes as necessary.

Format `clear ip ospf redistribution`

Mode Privileged EXEC

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 route can be `intra, inter, or external`. All the external type routes are given the same preference value. The range of *`preference`* value is 1 to 255.

Default 110

Format `distance ospf {intra-area` *`1–255`* `| inter-area` *`1–255`* `| external` *`1–255`*`}`

Mode Router OSPF Config

no distance ospf

This command sets the default route preference value of OSPF routes in the router. The type of OSPF can be intra, inter, or external. All the external type routes are given the same preference value.

Format `no distance ospf {`*`intra-area`* `|` *`inter-area`* `|` *`external`*`}`

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

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

passive-interface default (OSPF)

Use this command to enable global passive mode by default for all interfaces. It overrides any interface level passive mode. OSPF will not form adjacencies over a passive interface.

Default disabled

Format `passive-interface default`

Mode Router OSPF Config

no passive-interface default

Use this command to disable the global passive mode by default for all interfaces. Any interface previously configured to be passive reverts to non-passive mode.

Format `no passive-interface default`

Mode Router OSPF Config

passive-interface (OSPF)

Use this command to set the interface or tunnel as passive. It overrides the global passive mode that is currently effective on the interface or tunnel.

Default disabled

Format `passive-interface {slot/port | tunnel tunnel-id}`

Mode Router OSPF Config

no passive-interface

Use this command to set the interface or tunnel as non-passive. It overrides the global passive mode that is currently effective on the interface or tunnel.

Format `no passive-interface {slot/port | tunnel tunnel-id}`

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)

Use this command to enable individual OSPF traps, enable a group of trap flags at a time, or enable all the trap flags at a time. The different groups of trapflags, and each group's specific trapflags to enable or disable, are listed in Table 11.

Table 11: Trapflags Groups

Group	*Flags*
errors	• authentication-failure • bad-packet • config-error • virt-authentication-failure • virt-bad-packet • virt-config-error
if-rx	ir-rx-packet
lsa	• lsa-maxage • lsa-originate
overflow	• lsdb-overflow • lsdb-approaching-overflow
retransmit	• packets • virt-packets
rtb	• rtb-entry-info
state-change	• if-state-change • neighbor-state-change • virtif-state-change • virtneighbor-state-change

- To enable the individual flag, enter the `group name` followed by that particular flag.
- To enable all the flags in that group, give the group name followed by `all`.
- To enable all the flags, give the command as `trapflags all`.

Default disabled

Format
```
trapflags {
all | errors {all | authentication-failure | bad-packet | config-error | virt-
authentication-failure | virt-bad-packet | virt-config-error} |
if-rx {all | if-rx-packet} |
lsa {all | lsa-maxage | lsa-originate} |
overflow {all | lsdb-overflow | lsdb-approaching-overflow} |
retransmit {all | packets | virt-packets} |
rtb {all, rtb-entry-info} |
state-change {all | if-state-change | neighbor-state-change | virtif-state-change |
virtneighbor-state-change}
}
```

Mode Router OSPF Config

no trapflags

Use this command to revert to the default reference bandwidth.

- To disable the individual flag, enter the `group name` followed by that particular flag.
- To disable all the flags in that group, give the group name followed by `all`.
- To disable all the flags, give the command as `trapflags all`.

Format
```
no trapflags {
all |
errors {all | authentication-failure | bad-packet | config-error | virt-
authentication-failure | virt-bad-packet | virt-config-error} |
if-rx {all | if-rx-packet} |
lsa {all | lsa-maxage | lsa-originate} |
overflow {all | lsdb-overflow | lsdb-approaching-overflow} |
retransmit {all | packets | virt-packets} |
rtb {all, rtb-entry-info} |
state-change {all | if-state-change | neighbor-state-change | virtif-state-
change | virtneighbor-state-change}
}
```

Mode Router OSPF Config

OSPF Interface Commands

ip ospf area

Use this command to enable OSPFv2 and set the area ID of an interface or range of interfaces. The *area-id* is an IP address formatted as a 4-digit dotted-decimal number or a decimal value in the range of 0–4294967295. This command supersedes the effects of the `network area` command. It can also be used to configure the advertiseability of the secondary addresses on this interface into the OSPFv2 domain.

Default disabled

Format `ip ospf area` *area-id* `[secondaries none]`

Mode Interface Config

no ip ospf area

Use this command to disable OSPF on an interface.

Format `no ip ospf area [secondaries none]`

Mode Interface Config

bandwidth

By default, OSPF computes the link cost of an interface as the ratio of the reference bandwidth to the interface bandwidth. Reference bandwidth is specified with the `auto-cost` command. For the purpose of the OSPF link cost calculation, use the bandwidth command to specify the interface bandwidth. The bandwidth is specified in kilobits per second. If no bandwidth is configured, the bandwidth defaults to the actual interface bandwidth for port-based routing interfaces and to 10 Mbps for VLAN routing interfaces. This command does not affect the actual speed of an interface. You can use this command to configure a single interface or a range of interfaces.

Default actual interface bandwidth

Format `bandwidth` *1-10000000*

Mode Interface Config

no bandwidth

Use this command to set the interface bandwidth to its default value.

Format `no bandwidth`

Mode Interface Config

ip ospf authentication

This command sets the OSPF Authentication Type and Key for the specified interface or range of interfaces. 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 16 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. There is no default value for this command.

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 or range of interfaces. 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 or range of interfaces. 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 in seconds 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 or range of interfaces. 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 network

Use this command to configure OSPF to treat an interface or range of interfaces as a point-to-point rather than broadcast interface. The `broadcast` option sets the OSPF network type to broadcast. The `point-to-point` option sets the OSPF network type to point-to-point. OSPF treats interfaces as broadcast interfaces by default. (Loopback interfaces have a special loopback network type, which cannot be changed.) When there are only two routers on the network, OSPF can operate more efficiently by treating the network as a point-to-point network. For point-to-point networks, OSPF does not elect a designated router or generate a network link state advertisement (LSA). Both endpoints of the link must be configured to operate in point-to-point mode.

Default broadcast

Format `ip ospf network {broadcast | point-to-point}`

Mode Interface Config

no ip ospf network

Use this command to return the OSPF network type to the default.

Format `no ip ospf network`

Mode Interface Config

ip ospf priority

This command sets the OSPF priority for the specified router interface or range of interfaces. 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 or range of interfaces. 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 or range of interfaces. 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 on an interface or range of interfaces. 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

OSPF Graceful Restart Commands

The OSPF protocol can be configured to participate in the checkpointing service, so that these protocols can execute a *graceful restart* when the management unit fails. In a graceful restart, the hardware to continues forwarding IPv4 packets using OSPF routes while a backup switch takes over management unit responsibility

Graceful restart uses the concept of *helpful neighbors*. A fully adjacent router enters helper mode when it receives a link state announcement (LSA) from the restarting management unit indicating its intention of performing a graceful restart. In helper mode, a switch continues to advertise to the rest of the network that they have full adjacencies with the restarting router, thereby avoiding announcement of a topology change and and the potential for flooding of LSAs and shortest-path-first (SPF) runs (which determine OSPF routes). Helpful neighbors continue to forward packets through the restarting router. The restarting router relearns the network topology from its helpful neighbors.

Graceful restart can be enabled for either planned or unplanned restarts, or both. A planned restart is initiated by the operator through the management command `initiate failover`. The operator may initiate a failover in order to take the management unit out of service (for example, to address a partial hardware failure), to correct faulty system behavior which cannot be corrected through less severe management actions, or other reasons. An unplanned restart is an unexpected failover caused by a fatal hardware failure of the management unit or a software hang or crash on the management unit.

nsf

Use this command to enable the OSPF graceful restart functionality on an interface. To disable graceful restart, use the no form of the command.

Default Disabled

Format `nsf [ietf] [planned-only]`

Modes OSPF Router Configuration

Parameter	*Description*
ietf	This keyword is accepted but not required.
planned-only	This optional keyword indicates that OSPF should only perform a graceful restart when the restart is planned (i.e., when the restart is a result of the initiate failover command).

no nsf

Use this command to disable graceful restart for all restarts.

nsf restart-interval

Use this command to configure the number of seconds that the restarting router asks its neighbors to wait before exiting helper mode. This is referred to as the grace period. The restarting router includes the grace period in its grace LSAs. For planned restarts (using the `initiate failover` command), the grace LSAs are sent prior to restarting the management unit, whereas for unplanned restarts, they are sent after reboot begins.

The grace period must be set long enough to allow the restarting router to reestablish all of its adjacencies and complete a full database exchange with each of those neighbors.

Default 120 seconds

Format `nsf [ietf] restart-interval` *`1-1800`*

Modes OSPF Router Configuration

Parameter	*Description*
ietf	This keyword is accepted but not required.
seconds	The number of seconds that the restarting router asks its neighbors to wait before exiting helper mode. The range is from 1 to 1800 seconds.

no nsfrestart-interval

Use this command to revert the grace period to its default value.

Format `no [ietf] nsf restart-interval`

Modes OSPF Router Configuration

nsf helper

Use this command to enable helpful neighbor functionality for the OSPF protocol. You can enable this functionality for planned or unplanned restarts, or both.

Default OSPF may act as a helpful neighbor for both planned and unplanned restarts

Format `nsf helper [planned-only]`

Modes OSPF Router Configuration

Parameter	*Description*
planned-only	This optional keyword indicates that OSPF should only help a restarting router performing a planned restart.

no nsf helper

Use this command to disable helpful neighbor functionality for OSPF.

Format `no nsf helper`

Modes OSPF Router Configuration

nsf ietf helper disable

Use this command to disable helpful neighbor functionality for OSPF.

Note: The commands `no nsf helper` and `nsf ietf helper disable` are functionally equivalent. The command `nsf ietf helper disable` is supported solely for compatibility with other network software CLI.

Format `nsf ietf helper disable`

Modes OSPF Router Configuration

nsf helper strict-lsa-checking

The restarting router is unable to react to topology changes. In particular, the restarting router will not immediately update its forwarding table; therefore, a topology change may introduce forwarding loops or black holes that persist until the graceful restart completes. By exiting the graceful restart on a topology change, a router tries to eliminate the loops or black holes as quickly as possible by routing around the restarting router. A helpful neighbor considers a link down with the restarting router to be a topology change, regardless of the strict LSA checking configuration.

Use this command to require that an OSPF helpful neighbor exit helper mode whenever a topology change occurs.

Default Enabled.

Format `nsf [ietf] helper strict-lsa-checking`

Modes OSPF Router Configuration

Parameter	*Description*
ietf	This keyword is accepted but not required.

no nsf [ietf] helper strict-lsa-checking

Use this command to allow OSPF to continue as a helpful neighbor in spite of topology changes.

Default Enabled.

Format `nsf [ietf] helper strict-lsa-checking`

Modes OSPF Router Configuration

OSPF Show Commands

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.

Term	*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.
RFC 1583 Compatibility	Indicates whether 1583 compatibility is enabled or disabled. This is a configured value.
External LSDB Limit	The maximum number of non-default AS-external-LSA (link state advertisement) entries that can be stored in the link-state database.
Exit Overflow Interval	The number of seconds that, after entering overflow state, a router will attempt to leave overflow state.
Spf Delay Time	The number of seconds between two subsequent changes of LSAs, during which time the routing table calculation is delayed.
Spf Hold Time	The number of seconds between two consecutive spf calculations.
Opaque Capability	Shows whether the router is capable of sending Opaque LSAs. This is a configured value.
Autocost Ref BW	Shows the value of auto-cost reference bandwidth configured on the router.
Default Passive Setting	Shows whether the interfaces are passive by default.
Maximum Paths	The maximum number of paths that OSPF can report for a given destination.
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	The metric of the routes being redistributed. If the metric is not configured, this field is blank.
Metric Type	Shows whether the routes are External Type 1 or External Type 2.
Number of Active Areas	The number of active OSPF areas. An *active* OSPF area is an area with at least one interface up.
ABR Status	Shows whether the router is an OSPF Area Border Router.

Term	*Definition*
ASBR Status	Reflects whether the ASBR mode is enabled or disabled. Enable implies that the router is an autonomous system border router. The router automatically becomes an ASBR when it is configured to redistribute routes learnt from other protocols. The possible values for the ASBR status is enabled (if the router is configured to redistribute routes learned by other protocols) or disabled (if the router is not configured for the same).
Stub Router	When OSPF runs out of resources to store the entire link state database, or any other state information, OSPF goes into stub router mode. As a stub router, OSPF re-originates its own router LSAs, setting the cost of all non-stub interfaces to infinity. To restore OSPF to normal operation, disable and re-enable OSPF.
External LSDB Overflow	When the number of non-default external LSAs exceeds the configured limit, External LSDB Limit, OSPF goes into LSDB overflow state. In this state, OSPF withdraws all of its self-originated non-default external LSAs. After the Exit Overflow Interval, OSPF leaves the overflow state, if the number of external LSAs has been reduced.
External LSA Count	The number of external (LS type 5) link-state advertisements in the link-state database.
External LSA Checksum	The sum of the LS checksums of external link-state advertisements contained in the link-state database.
AS_OPAQUE LSA Count	Shows the number of AS Opaque LSAs in the link-state database.
AS_OPAQUE LSA Checksum	Shows the sum of the LS Checksums of AS Opaque LSAs contained in the link-state database.
New LSAs Originated	The number of new link-state advertisements that have been originated.
LSAs Received	The number of link-state advertisements received determined to be new instantiations.
LSA Count	The total number of link state advertisements currently in the link state database.
Maximum Number of LSAs	The maximum number of LSAs that OSPF can store.
LSA High Water Mark	The maximum size of the link state database since the system started.
Retransmit List Entries	The total number of LSAs waiting to be acknowledged by all neighbors. An LSA may be pending acknowledgment from more than one neighbor.
Maximum Number of Retransmit Entries	The maximum number of LSAs that can be waiting for acknowledgment at any given time.
NSF Support	Indicates whether nonstop forwarding (NSF) is enabled for the OSPF protocol for planned restarts, unplanned restarts or both (*AIways*).
NSF Restart Interval	The user-configurable grace period during which a neighboring router will be in the helper state after receiving notice that the management unit is performing a graceful restart.
NSF Restart Status	The current graceful restart status of the router. • Not Restarting • Planned Restart • Unplanned Restart
NSF Restart Age	Number of seconds until the graceful restart grace period expires.

Term	*Definition*
NSF Restart Exit Reason	Indicates why the router last exited the last restart: • None — Graceful restart has not been attempted. • In Progress — Restart is in progress. • Completed — The previous graceful restart completed successfully. • Timed Out — The previous graceful restart timed out. • Topology Changed — The previous graceful restart terminated prematurely because of a topology change.
NSF Help Support	Indicates whether helpful neighbor functionality has been enabled for OSPF for planned restarts, unplanned restarts, or both (Always).
NSF help Strict LSA checking	Indicates whether strict LSA checking has been enabled. If enabled, then an OSPF helpful neighbor will exit helper mode whenever a topology change occurs. If disabled, an OSPF neighbor will continue as a helpful neighbor in spite of topology changes.

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

```
(alpha2) #show ip ospf

Router ID.....................................2.2.2.2
OSPF Admin Mode...............................Disable
RFC 1583 Compatibility........................Enable
External LSDB Limit...........................No Limit
Exit Overflow Interval........................0
Spf Delay Time................................5
Spf Hold Time.................................10
Opaque Capability.............................Disable
AutoCost Ref BW...............................100 Mbps
Default Passive Setting.......................Disabled
Maximum Paths.................................4
Default Metric................................Not configured

Default Route Advertise.......................Disabled
Always........................................FALSE
Metric........................................Not configured
Metric Type...................................External Type 2


Number of Active Areas........................ 3 (3 normal, 0 stub, 0 nssa)
ABR Status....................................Disable
ASBR Status...................................Disable
Stub Router...................................FALSE
External LSDB Overflow........................FALSE
External LSA Count............................0
External LSA Checksum.........................0
AS_OPAQUE LSA Count...........................0
AS_OPAQUE LSA Checksum........................0
LSAs Originated...............................0
LSAs Received.................................0
LSA Count.....................................0
Maximum Number of LSAs........................18200
LSA High Water Mark...........................0
Retransmit List Entries....................... 9078
Maximum Number of Retransmit Entries........... 72800
```

```
Retransmit Entries High Water Mark..... 72849
NSF Support..................................... Always
NSF Restart Interval............................ 120 seconds
NSF Restart Status.............................. Not restarting
NSF Restart Age................................. 0
NSF Restart Exit Reason......................... Completed
NSF Helper Support.............................. Always
NSF Helper Strict LSA checking.................. Enabled
```

show ip ospf abr

This command displays the internal OSPF routing table entries to Area Border Routers (ABR). This command takes no options.

Format `show ip ospf abr`

Mode
- Privileged EXEC
- User EXEC

Term	*Definition*
Type	The type of the route to the destination. It can be either: • 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.
Next Hop	Next hop toward the destination.
Next Hop Intf	The outgoing router interface to use when forwarding traffic to the next hop.

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

Term	*Definition*
AreaID	The area id of the requested OSPF area.
External Routing	A number representing the external routing capabilities for this area.
Spf Runs	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	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:

Term	*Definition*
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	The metric value for the default route advertised into the NSSA.
Default Metric Type	The metric type for the default route advertised into the NSSA.
Translator Role	The NSSA translator role of the ABR, which is always or candidate.
Translator Stability Interval	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 asbr

This command displays the internal OSPF routing table entries to Autonomous System Boundary Routers (ASBR). This command takes no options.

Format `show ip ospf asbr`

Mode
- Privileged EXEC
- User EXEC

Term	*Definition*
Type	The type of the route to the destination. It can be 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.
Next Hop	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.

Format `show ip ospf [areaid] database [{database-summary | [{asbr-summary | external | network | nssa-external | opaque-area | opaque-as | opaque-link | router | summary}] [lsid] [{adv-router [ipaddr] | self-originate}]}]`

Mode
- Privileged EXEC
- User EXEC

The information below is only displayed if OSPF is enabled.

Parameter	*Description*
asbr-summary	Use *asbr-summary* to show the autonomous system boundary router (ASBR) summary LSAs.
external	Use *external* to display the external LSAs.
network	Use *network* to display the network LSAs.
nssa-external	Use *nssa-external* to display NSSA external LSAs.
opaque-area	Use *opaque-area* to display area opaque LSAs.
opaque-as	Use *opaque-as* to display AS opaque LSAs.
opaque-link	Use *opaque-link* to display link opaque LSAs.
router	Use *router* to display router LSAs.

Parameter	*Description*
summary	Use *summary* to show the LSA database summary information.
lsid	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.
adv-router	Use *adv-router* to show the LSAs that are restricted by the advertising router.
self-originate	Use *self-originate* to display the LSAs in that are self originated. The information below is only displayed if OSPF is enabled

For each link-type and area, the following information is displayed:

Term	*Definition*
Link Id	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	A number representing the age of the link state advertisement in seconds.
Sequence	A number that represents which LSA is more recent.
Checksum	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

Term	*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 OSPF 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.
Opaque AS	Number of opaque AS LSAs in the database.
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`*`}`

Mode
- Privileged EXEC
- User EXEC

Term	*Definition*
IP Address	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.
Secondary IP Address(es)	The secondary IP addresses if any are configured on the interface.
OSPF Admin Mode	States whether OSPF is enabled or disabled on a router interface.
OSPF Area ID	The OSPF Area ID for the specified interface.
OSPF Network Type	The type of network on this interface that the OSPF is running on.
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 Acknowledgment Interval for the specified interface.
Transmit Delay	A number representing the OSPF Transmit Delay Interval for the specified interface.
Authentication Type	The OSPF Authentication Type for the specified interface are: none, simple, and encrypt.
Metric Cost	The cost of the OSPF interface.
Passive Status	Shows whether the interface is passive or not.
OSPF MTU-ignore	Indicates whether to ignore MTU mismatches in database descriptor packets sent from neighboring routers.

The information below will only be displayed if OSPF is enabled.

Term	*Definition*
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.
Local Link LSAs	The number of Link Local Opaque LSAs in the link-state database.
Local Link LSA Checksum	The sum of LS Checksums of Link Local Opaque LSAs in the link-state database.

Example: The following shows example CLI display output for the command when the OSPF Admin Mode is disabled.

```
(Routing) >show ip ospf interface 1/0/1

IP Address..................................... 0.0.0.0
Subnet Mask.................................... 0.0.0.0
Secondary IP Address(es).......................
OSPF Admin Mode................................ Disable
OSPF Area ID................................... 0.0.0.0
OSPF Network Type.............................. Broadcast
Router Priority................................ 1
Retransmit Interval............................ 5
Hello Interval................................. 10
Dead Interval.................................. 40
LSA Ack Interval............................... 1
Transmit Delay................................. 1
Authentication Type............................ None
Metric Cost.................................... 1  (computed)
Passive Status................................. Non-passive interface
OSPF Mtu-ignore................................ Disable

OSPF is not enabled on this interface.

(Routing) #
```

show ip ospf interface brief

This command displays brief information for the IFO object or virtual interface tables.

Format `show ip ospf interface brief`

Mode
- Privileged EXEC
- User EXEC

Term	*Definition*
Interface	*slot/port*
OSPF Admin Mode	States whether OSPF is enabled or disabled on a router interface.
OSPF Area ID	The OSPF Area Id for the specified interface.
Router Priority	A number representing the OSPF Priority for the specified interface.
Cost	The metric cost of the OSPF 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.
Interface Transmit Delay	A number representing the OSPF Transmit Delay for the specified interface.
LSA Ack Interval	A number representing the OSPF LSA Acknowledgment 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

Term	*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.
Sent Packets	The number of OSPF packets transmitted on the interface.
Received Packets	The number of valid OSPF packets received on the interface.
Discards	The number of received OSPF packets discarded because of an error in the packet or an error in processing the packet.
Bad Version	The number of received OSPF packets whose version field in the OSPF header does not match the version of the OSPF process handling the packet.
Source Not On Local Subnet	The number of received packets discarded because the source IP address is not within a subnet configured on a local interface. ***Note:*** This field applies only to OSPFv2.
Virtual Link Not Found	The number of received OSPF packets discarded where the ingress interface is in a non-backbone area and the OSPF header identifies the packet as belonging to the backbone, but OSPF does not have a virtual link to the packet's sender.
Area Mismatch	The number of OSPF packets discarded because the area ID in the OSPF header is not the area ID configured on the ingress interface.
Invalid Destination Address	The number of OSPF packets discarded because the packet's destination IP address is not the address of the ingress interface and is not the AllDrRouters or AllSpfRouters multicast addresses.
Wrong Authentication Type	The number of packets discarded because the authentication type specified in the OSPF header does not match the authentication type configured on the ingress interface. ***Note:*** This field applies only to OSPFv2.
Authentication Failure	The number of OSPF packets dropped because the sender is not an existing neighbor or the sender's IP address does not match the previously recorded IP address for that neighbor. ***Note:*** This field applies only to OSPFv2.

Term	*Definition*
No Neighbor at Source Address	The number of OSPF packets dropped because the sender is not an existing neighbor or the sender's IP address does not match the previously recorded IP address for that neighbor. ***Note:*** Does not apply to Hellos.
Invalid OSPF Packet Type	The number of OSPF packets discarded because the packet type field in the OSPF header is not a known type.
Hellos Ignored	The number of received Hello packets that were ignored by this router from the new neighbors after the limit has been reached for the number of neighbors on an interface or on the system as a whole.

Table 12 lists the number of OSPF packets of each type sent and received on the interface.

Table 12: Type of OSPF Packets Sent and Received on the Interface

Packet Type	*Sent*	*Received*
Hello	6960	6960
Database Description	3	3
LS Request	1	1
LS Update	141	42
LS Acknowledgment	40	135

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:

Term	*Definition*
Router ID	The 4-digit dotted-decimal number of the neighbor router.
Priority	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	The IP address of the neighbor.
Interface	The interface of the local router in slot/port format.

Term	*Definition*
State	The state of the neighboring routers. Possible values are: • 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	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:

Term	*Definition*
Interface	*slot/port*
Neighbor IP Address	The IP address of the neighbor router.
Interface Index	The interface ID of the neighbor router.
Area ID	The area ID of the OSPF area associated with the interface.
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	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	The amount of time, in seconds, to wait before the router assumes the neighbor is unreachable.
Up Time	Neighbor uptime; how long since the adjacency last reached the Full state.
State	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	An integer representing the current length of the retransmission queue of the specified neighbor router Id of the specified interface.

Term	*Definition*
Restart Helper Status	Indicates the status of this router as a helper during a graceful restart of the router specified in the command line: • Helping—This router is acting as a helpful neighbor to this neighbor. A helpful neighbor does not report an adjacency change during graceful restart, but continues to advertise the restarting router as a FULL adjacency. A helpful neighbor continues to forward data packets to the restarting router, trusting that the restarting router's forwarding table is maintained during the restart. • Not Helping—This router is not a helpful neighbor at this time.
Restart Reason	When this router is in helpful neighbor mode, this indicates the reason for the restart as provided by the restarting router: • Unknown (0) • Software restart (1) • Software reload/upgrade (2) • Switch to redundant control processor (3) • Unrecognized - a value not defined in RFC 3623 When DWS-4000 sends a grace LSA, it sets the Restart Reason to Software Restart on a planned warm restart (when the `initiate failover` command is invoked), and to Unknown on an unplanned warm restart.
Remaining Grace Time	The number of seconds remaining the in current graceful restart interval. This is displayed only when this router is currently acting as a helpful neighbor for the router specified in the command.
Restart Helper Exit Reason	Indicates the reason that the specified router last exited a graceful restart. • None—Graceful restart has not been attempted • In Progress—Restart is in progress • Completed—The previous graceful restart completed successfully • Timed Out—The previous graceful restart timed out • Topology Changed—The previous graceful restart terminated prematurely because of a topology change

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

```
(alpha1) #show ip ospf neighbor 170.1.1.50

Interface.....................................0/17
Neighbor IP Address...........................170.1.1.50
Interface Index...............................17
Area Id.......................................0.0.0.2
Options.......................................0x2
Router Priority...............................1
Dead timer due in (secs)......................15
Up Time.......................................0 days 2 hrs 8 mins 46 secs
State.........................................Full/BACKUP-DR
Events........................................4
Retransmission Queue Length...................0
Restart Helper Status..........................  Helping
Restart Reason.................................  Software Restart (1)
Remaining Grace Time...........................  10 sec
Restart Helper Exit Reason.....................  In Progress
```

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

Term	*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

Term	*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

Term	*Definition*
Area ID	A 32-bit identifier for the created stub area.
Type of Service	The type of service associated with the stub metric. DWS-4000 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

Term	*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.
Interface Transmit Delay	The configured transmit delay for the OSPF virtual interface.
Retransmit Interval	The configured retransmit interval for the OSPF virtual interface.
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

Term	*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.
Transmit Delay	The configured transmit delay for the OSPF virtual interface.

Routing Information Protocol Commands

This section describes the commands you use to view and configure Routing Information Protocol (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 or range of interfaces.

Default disabled

Format `ip rip`

Mode Interface Config

no ip rip

This command disables RIP on a router interface.

Format `no ip rip`

Mode Interface Config

auto-summary

This command enables the RIP auto-summarization mode.

Default disabled

Format `auto-summary`

Mode Router RIP Config

no auto-summary

This command disables the RIP auto-summarization mode.

Format `no auto-summary`

Mode Router RIP Config

default-information originate (RIP)

This command is used to control the advertisement of default routes.

Format `default-information originate`

Mode Router RIP Config

no default-information originate (RIP)

This command is used to control the advertisement of default routes.

Format `no default-information originate`

Mode Router RIP Config

default-metric (RIP)

This command is used to set a default for the metric of distributed routes.

Format `default-metric 0-15`

Mode Router RIP Config

no default-metric (RIP)

This command is used to reset the default metric of distributed routes to its default value.

Format `no default-metric`

Mode Router RIP Config

distance rip

This command sets the route preference value of RIP in the router. Lower route preference values are preferred when determining the best route. A route with a preference of 255 cannot be used to forward traffic.

Default 15

Format `distance rip 1-255`

Mode Router RIP Config

no distance rip

This command sets the default route preference value of RIP in the router.

Format `no distance rip`

Mode Router RIP Config

distribute-list out (RIP)

This command is used to specify the access list to filter routes received from the source protocol.

Default 0

Format `distribute-list 1-199 out {ospf | bgp | static | connected}`

Mode Router RIP Config

no distribute-list out

This command is used to specify the access list to filter routes received from the source protocol.

Format `no distribute-list 1-199 out {ospf | bgp | static | connected}`

Mode Router RIP Config

ip rip authentication

This command sets the RIP Version 2 Authentication Type and Key for the specified interface or range of interfaces. The value of *type* is either `none, simple, or encrypt`. The value for authentication key *[key]* must be 16 bytes or less. The *[key]* is composed of standard displayable, 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 an interface or range of interfaces to allow RIP control packets of the specified version(s) to be received.

The value for *mode* is one of: `rip1` to receive only RIP version 1 formatted packets, `rip2` for RIP version 2, `both` to receive packets from either format, or `none` to not allow any RIP control packets to be received.

Default both

Format `ip rip receive version {rip1 | rip2 | both | none}`

Mode Interface Config

no ip rip receive version

This command configures the interface to allow RIP control packets of the default version(s) to be received.

Format `no ip rip receive version`

Mode Interface Config

ip rip send version

This command configures an interface or range of interfaces to allow RIP control packets of the specified version to be sent. The value for *mode* is one of: `rip1` to broadcast RIP version 1 formatted packets, `rip1c` (RIP version 1 compatibility mode) which sends RIP version 2 formatted packets via broadcast, `rip2` for sending RIP version 2 using multicast, or `none` to not allow any RIP control packets to be sent.

Default ripi2

Format `ip rip send version {rip1 | rip1c | rip2 | none}`

Mode Interface Config

no ip rip send version

This command configures the interface to allow RIP control packets of the default version to be sent.

Format `no ip rip send version`

Mode Interface Config

hostroutesaccept

This command enables the RIP hostroutesaccept mode.

Default enabled

Format `hostroutesaccept`

Mode Router RIP Config

no hostroutesaccept

This command disables the RIP hostroutesaccept mode.

Format `no hostroutesaccept`

Mode Router RIP Config

split-horizon

This command sets the RIP split horizon mode. Split horizon is a technique for avoiding problems caused by including routes in updates sent to the router from which the route was originally learned. The options are:

- None - no special processing for this case.
- Simple - a route will not be included in updates sent to the router from which it was learned.
- Poisoned reverse - a route will be included in updates sent to the router from which it was learned, but the metric will be set to infinity.

Default simple

Format `split-horizon {none | simple | poison}`

Mode Router RIP Config

no split-horizon

This command sets the default RIP split horizon mode.

Format `no split-horizon`

Mode Router RIP Config

redistribute (RIP)

This command configures RIP protocol to redistribute routes from the specified source protocol/routers. There are five possible match options. When you submit the command redistribute ospf match *match-type* the match-type or types specified are added to any match types presently being redistributed. Internal routes are redistributed by default.

Default
- metric—not-configured
- match—internal

Format for OSPF as source protocol
`redistribute ospf [metric 0-15] [match [internal] [external 1] [external 2] [nssa-external 1] [nssa-external-2]]`

Format for other source protocol
`redistribute {bgp | static | connected} [metric 0-15]`

Mode Router RIP Config

no redistribute

This command de-configures RIP protocol to redistribute routes from the specified source protocol/routers.

Format
`no redistribute {ospf | bgp | static | connected} [metric] [match [internal] [external 1] [external 2] [nssa-external 1] [nssa-external-2]]`

Mode Router RIP Config

show ip rip

This command displays information relevant to the RIP router.

Format
`show ip rip`

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
RIP Admin Mode	Enable or disable.
Split Horizon Mode	None, simple or poison reverse.
Auto Summary Mode	Enable or disable. If enabled, groups of adjacent routes are summarized into single entries, in order to reduce the total number of entries The default is enable.
Host Routes Accept Mode	Enable or disable. If enabled the router accepts host routes. The default is enable.
Global Route Changes	The number of route changes made to the IP Route Database by RIP. This does not include the refresh of a route's age.
Global queries	The number of responses sent to RIP queries from other systems.
Default Metric	The default metric of redistributed routes if one has already been set, or blank if not configured earlier. The valid values are 1 to 15.
Default Route Advertise	The default route.

show ip rip interface brief

This command displays general information for each RIP interface. For this command to display successful results routing must be enabled per interface (i.e., ip rip).

Format `show ip rip interface brief`

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
Interface	*slot/port*
IP Address	The IP source address used by the specified RIP interface.
Send Version	The RIP version(s) used when sending updates on the specified interface. The types are none, RIP-1, RIP-1c, RIP-2
Receive Version	The RIP version(s) allowed when receiving updates from the specified interface. The types are none, RIP-1, RIP-2, Both
RIP Mode	The administrative mode of router RIP operation (enabled or disabled).
Link State	The mode of the interface (up or down).

show ip rip interface

This command displays information related to a particular RIP interface.

Format `show ip rip interface slot/port`

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
Interface	slot/port - This is a configured value.
IP Address	The IP source address used by the specified RIP interface. This is a configured value.
Send Version	The RIP version(s) used when sending updates on the specified interface. The types are none, RIP-1, RIP-1c, RIP-2. This is a configured value.
Receive Version	The RIP version(s) allowed when receiving updates from the specified interface. The types are none, RIP-1, RIP-2, Both. This is a configured value.
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.

Term	*Definition*
Bad Packets Received	The number of RIP response packets received by the RIP process which were subsequently discarded for any reason.
Bad Routes Received	The number of routes contained in valid RIP packets that were ignored for any reason.
Updates Sent	The number of triggered RIP updates actually sent on this interface.

ICMP Throttling Commands

This section describes the commands you use to configure options for the transmission of various types of ICMP messages.

ip unreachables

Use this command to enable the generation of ICMP Destination Unreachable messages on an interface or range of interfaces. By default, the generation of ICMP Destination Unreachable messages is enabled.

Default enable

Format `ip unreachables`

Mode Interface Config

no ip unreachables

Use this command to prevent the generation of ICMP Destination Unreachable messages.

Format `no ip unreachables`

Mode Interface Config

ip redirects

Use this command to enable the generation of ICMP Redirect messages by the router. By default, the generation of ICMP Redirect messages is enabled. You can use this command to configure an interface, a range of interfaces, or all interfaces.

Default enable

Format `ip redirects`

Mode
- Global Config
- Interface Config

no ip redirects

Use this command to prevent the generation of ICMP Redirect messages by the router.

Format `no ip redirects`

Mode
- Global Config
- Interface Config

ip icmp echo-reply

Use this command to enable the generation of ICMP Echo Reply messages by the router. By default, the generation of ICMP Echo Reply messages is enabled.

Default enable

Format `ip icmp echo-reply`

Mode Global Config

no ip icmp echo-reply

Use this command to prevent the generation of ICMP Echo Reply messages by the router.

Format `no ip icmp echo-reply`

Mode Global Config

ip icmp error-interval

Use this command to limit the rate at which IPv4 ICMP error messages are sent. The rate limit is configured as a token bucket, with two configurable parameters, *burst-size* and *burst-interval*.

The *burst-interval* specifies how often the token bucket is initialized with *burst-size* tokens. *burst-interval* is from 0 to 2147483647 milliseconds (msec). The *burst-size* is the number of ICMP error messages that can be sent during one *burst-interval*. The range is from 1 to 200 messages. To disable ICMP rate limiting, set *burst-interval* to zero (0).

Default
- *burst-interval* of 1000 msec.
- *burst-size* of 100 messages

Format `ip icmp error-interval` *`burst-interval [burst-size]`*

Mode Global Config

no ip icmp error-interval

Use the **no** form of the command to return *burst-interval* and *burst-size* to their default values.

Format `no ip icmp error-interval`

Mode Global Config

Section 7: IPv6 Commands

This chapter describes the IPv6 commands available in the DWS-4000 CLI.

This chapter contains the following sections:

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

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

IPv6 Management Commands

IPv6 Management commands allow a device to be managed via an IPv6 address in a switch or IPv4 routing (i.e., independent from the IPv6 Routing package). For Routing/IPv6 builds of DWS-4000 dual IPv4/IPv6 operation over the service port is enabled. DWS-4000 has capabilities such as:

- Static assignment of IPv6 addresses and gateways for the service/network ports.
- The ability to ping an IPv6 link-local address over the service/network port.
- Using IPv6 Management commands, you can send SNMP traps and queries via the service/network port.
- The user can manage a device via the network port (in addition to a Routing Interface or the Service port).

serviceport ipv6 enable

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

Default enabled

Format `serviceport ipv6 enable`

Mode Privileged EXEC

no serviceport ipv6 enable

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

Format `no serviceport ipv6 enable`

Mode Privileged EXEC

network ipv6 enable

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

Default enabled

Format `network ipv6 enable`

Mode Privileged EXEC

no network ipv6 enable

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

Format `no network ipv6 enable`

Mode Privileged EXEC

serviceport ipv6 address

Use the options of this command to manually configure IPv6 global address, enable/disable stateless global address autoconfiguration and to enable/disable dhcpv6 client protocol information on the service port.

Note: Multiple IPv6 prefixes can be configured on the service port.

Format `serviceport ipv6 address {address/prefix-length [eui64]|autoconfig|dhcp}`

Mode Privileged EXEC

Parameter	*Description*
address	IPv6 prefix in IPv6 global address format.
prefix-length	IPv6 prefix length value.
eui64	Formulate IPv6 address in eui64 address format.
autoconfig	Configure stateless global address autoconfiguration capability.
dhcp	Configure dhcpv6 client protocol.

no serviceport ipv6 address

Use the command `no serviceport ipv6 address` to remove all configured IPv6 prefixes on the service port interface. Use the command with the *address* option to remove the manually configured IPv6 global address on the network port interface. Use the command with the `autoconfig` option to disable the stateless global address autoconfiguration on the service port.

Use the command with the `dhcp` option to disable the DHCPv6 client protocol on the service port.

Format `no serviceport ipv6 address {address/prefix-length [eui64] | autoconfig | dhcp}`

Mode Privileged EXEC

serviceport ipv6 gateway

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

.

Note: Only a single IPv6 gateway address can be configured for the service port. There may be a combination of IPv6 prefixes and gateways that are explicitly configured and those that are set through auto-address configuration with a connected IPv6 router on their service port interface.

Format `serviceport ipv6 gateway` *`gateway-address`*

Mode Privileged EXEC

Parameter	*Description*
gateway-address	Gateway address in IPv6 global or link-local address format.

no serviceport ipv6 gateway

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

Format `no serviceport ipv6 gateway`

Mode Privileged EXEC

network ipv6 address

Use the options of this command to manually configure IPv6 global address, enable/disable stateless global address autoconfiguration and to enable/disable dhcpv6 client protocol information for the network port. Multiple IPv6 addresses can be configured on the network port.

Format `network ipv6 address {`*`address/prefix-length`* `[eui64] | autoconfig | dhcp}`

Mode Privileged EXEC

Parameter	*Description*
address	IPv6 prefix in IPv6 global address format.
prefix-length	IPv6 prefix length value.
eui64	Formulate IPv6 address in eui64 format.
autoconfig	Configure stateless global address autoconfiguration capability.
dhcp	Configure dhcpv6 client protocol.

no network ipv6 address

The command `no network ipv6 address` removes all configured IPv6 prefixes. Use this command with the *`address`* option to remove the manually configured IPv6 global address on the network port interface. Use this command with the `autoconfig` option to disable the stateless global address autoconfiguration on the network port. Use this command with the `dhcp` option disables the DHCPv6 client protocol on the network port.

Format `no network ipv6 address {address/prefix-length [eui64] | autoconfig | dhcp}`

Mode Privileged EXEC

network ipv6 gateway

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

Format `network ipv6 gateway gateway-address`

Mode Privileged EXEC

Parameter	*Description*
gateway-address	Gateway address in IPv6 global or link-local address format.

no network ipv6 gateway

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

Format `no network ipv6 gateway`

Mode Privileged EXEC

show network ndp

This command displays NDP cache information for the network port.

Default enabled

Format `show network ndp`

Mode
- Privileged EXEC
- User EXEC

Field	*Description*
IPv6 Address	The IPv6 address of the interface.
MAC Address	The MAC Address used.
isRtr	Specifies the router flag.
Neighbor State	The state of the neighbor cache entry. Possible values are: Reachable, Delay.
Age Updated	The time in seconds that has elapsed since an entry was added to the cache.

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

```
(admin) #show network ndp
                                                        Neighbor       Age
IPv6 Address                 MAC Address      isRtr       State       Updated
-------------------------- ----------------- -----       --------    -------
3017::204:76FF:FE73:423A  00:04:76:73:42:3a               Reachable 447535
FE80::204:76FF:FE73:423A  00:04:76:73:42:3a                   Delay  447540
```

show serviceport ndp

Use this command to display the neighbor entries cached on the service port.

Default enabled

Format `show serviceport ndp`

Mode
- Privileged EXEC
- User EXEC

Field	*Description*
IPv6 Address	The IPv6 address of the neighbor.
MAC Address	The MAC address of the neighbor.
State	The state of the neighbor cache entry.
Last Updated	The time in seconds that has elapsed since an entry was added to the cache.

ping ipv6

Use this command to determine whether another computer is on the network. Ping provides a synchronous response when initiated from the CLI and Web interfaces. To use the command, configure the switch for network (in-band) connection. The source and target devices must have the ping utility enabled and running on top of TCP/IP. The switch can be pinged from any IP workstation with which the switch is connected through the default VLAN (VLAN 1), as long as there is a physical path between the switch and the workstation. The terminal interface sends three pings to the target station. Use the *ipv6-address|hostname* parameter to ping an interface by using the global IPv6 address of the interface. Use the optional *size* keyword to specify the size of the ping packet.

You can utilize the ping or traceroute facilities over the service/network ports when using an IPv6 global address *ipv6-global-address|hostname*. Any IPv6 global address or gateway assignments to these interfaces will cause IPv6 routes to be installed within the IP stack such that the ping or traceroute request is routed out the service/network port properly. When referencing an IPv6 link-local address, you must also specify the service or network port interface by using the `serviceport` or `network` parameter.

Default
- The default count is 1.
- The default interval is 3 seconds.
- The default size is 0 bytes.

Format `ping ipv6 {`*ipv6-global-address|hostname* `| {interface {slot/port | serviceport | network}` *link-local-address*`} [size` *datagram-size]*`}`

Mode
- Privileged EXEC
- User Exec

ping ipv6 interface

Use this command to determine whether another computer is on the network. To use the command, configure the switch for network (in-band) connection. The source and target devices must have the ping utility enabled and running on top of TCP/IP. The switch can be pinged from any IP workstation with which the switch is connected through the default VLAN (VLAN 1), as long as there is a physical path between the switch and the workstation. The terminal interface sends three pings to the target station. Use the *interface* keyword to ping an interface by using the link-local address or the global IPv6 address of the interface. You can use a loopback, network port, serviceport, tunnel, or physical interface as the source. Use the optional `size` keyword to specify the size of the ping packet. The *ipv6-address* is the link local IPv6 address of the device you want to query.

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

Modes
- 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

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 406. To assign an IPv6 address to the tunnel interface, see “ipv6 address” on page 499.

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. With the optional 6to4 argument, the tunnel mode is set to 6to4 automatic. Without the optional 6to4 argument, the tunnel mode is configured.

Format `tunnel mode ipv6ip [6to4]`

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:

Term	*Definition*
Tunnel ID	The tunnel identification number.
Interface	The name of the tunnel interface.
Tunnel Mode	The tunnel mode.
Source Address	The source transport address of the tunnel.
Destination Address	The destination transport address of the tunnel.

If you specify a tunnel ID, the command shows the following information for the tunnel:

Term	*Definition*
Interface Link Status	Shows whether the link is up or down.
MTU Size	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 406. To assign an IPv6 address to the loopback interface, see “ipv6 address” on page 499.

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:

Term	*Definition*
Loopback ID	The loopback ID associated with the rest of the information in the row.
Interface	The interface name.
IP Address	The IPv4 address of the interface.
Received Packets	The number of packets received on this interface.
Sent Packets	The number of packets transmitted from this interface.
IPv6 Address	The IPv6 address of this interface.

If you specify a loopback ID, the following information appears:

Term	*Definition*
Interface Link Status	Shows whether the link is up or down.
IP Address	The IPv4 address of the interface.
IPv6 is enabled (disabled)	Shows whether IPv6 is enabled on the interface.
IPv6 Address/ Length is	The IPv6 address of the interface.
MTU size	The maximum transmission size for packets on this interface, in bytes.

IPv6 Routing Commands

This section describes the IPv6 commands 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 hop-limit

This command defines the unicast hop count used in ipv6 packets originated by the node. The value is also included in router advertisements. Valid values for *hops* are 1–64 inclusive. The default *not configured* means that a value of zero is sent in router advertisements and a value of 64 is sent in packets originated by the node. Note that this is not the same as configuring a value of 64.

Default not configured

Format `ipv6 hop-limit` *hops*

Mode Global Config

no ipv6 hop-limit

This command returns the unicast hop count to the default.

Format `no ipv6 hop-limit`

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 or range of interfaces, 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 or range of interfaces, 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 address dhcp

This command enables the DHCPv6 client on an in-band interface so that it can acquire network information, such as the IPv6 address, from a network DHCP server.

Default disabled

Format `ipv6 address dhcp`

Mode Interface Config

no ipv6 address dhcp

This command releases a leased address and disables DHCPv6 on an interface.

Format `no ipv6 address dhcp`

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. Specifying `Null0` as nexthop parameter adds a static reject route. 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. You can specify a slot/port or `tunnel` *tunnel_id* interface to identify direct static routes from point-to-point and broadcast interfaces. The interface 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* | `Null0` | `interface` {slot/port | `tunnel` *tunnel_id*} *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 the preference of a route to the default preference.

Format `no ipv6 route` *ipv6-prefix/prefix_length* [{*next-hop-address* | `Null0` | `interface` {slot/port | `tunnel` *tunnel_id*} *next-hop-address* | *preference*}]

Mode Global Config

ipv6 route distance

This command sets the default distance (preference) for IPv6 static routes. Lower route distance values are preferred when determining the best route. The `ipv6 route` command allows you to optionally set the distance (preference) of an individual static route. The default distance is used when no distance is specified in this command.

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 `ipv6 route distance` command.

Default	1
Format	`ipv6 route distance` *`1-255`*
Mode	Global Config

no ipv6 route distance

This command resets the default static route preference value in the router to the original default preference. Lower route preference values are preferred when determining the best route.

Format	`no ipv6 route distance`
Mode	Global Config

ipv6 mtu

This command sets the maximum transmission unit (MTU) size, in bytes, of IPv6 packets on an interface or range of interfaces. 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 on an interface or range of interfaces. 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 on the interface or range of interfaces. 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. This command can configure a single interface or a range of interfaces.

Default 0

Format `ipv6 nd ns-interval {1000-4294967295 | 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 on the interface or range of interfaces.

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 or range of interfaces. 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. This command can configure a single interface or a range of interfaces.

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 or range of interfaces.

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

Use the `ipv6 nd prefix` command to configure parameters associated with prefixes the router advertises in its router advertisements. 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.

This command can be used to configure a single interface or a range of interfaces.

The router advertises its global IPv6 prefixes in its router advertisements (RAs). An RA only includes the prefixes of the IPv6 addresses configured on the interface where the RA is transmitted. Addresses are configured using the `ipv6 address` interface configuration command. Each prefix advertisement includes information about the prefix, such as its lifetime values and whether hosts should use the prefix for on-link determination or address auto-configuration. Use the `ipv6 nd prefix` command to configure these values.

The `ipv6 nd prefix` command allows you to preconfigure RA prefix values before you configure the associated interface address. In order for the prefix to be included in RAs, you must configure an address that matches the prefix using the `ipv6 address` command. Prefixes specified using `ipv6 nd prefix` without associated interface address will not be included in RAs and will not be committed to the device configuration.

Default
- valid-lifetime—2592000
- preferred-lifetime— 604800
- 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

no ipv6 nd prefix

This command sets prefix configuration to default values.

Format `no ipv6 nd prefix` *`prefix/prefix_length`*

Mode Interface Config

ipv6 unreachables

Use this command to enable the generation of ICMPv6 Destination Unreachable messages on the interface or range of interfaces. By default, the generation of ICMPv6 Destination Unreachable messages is enabled.

Default enable

Format `ipv6 unreachables`

Mode Interface Config

no ipv6 unreachables

Use this command to prevent the generation of ICMPv6 Destination Unreachable messages.

Format `no ipv6 unreachables`

Mode Interface Config

ipv6 icmp error-interval

Use this command to limit the rate at which ICMPv6 error messages are sent. The rate limit is configured as a token bucket, with two configurable parameters, *burst-size* and *burst-interval*.

The *burst-interval* specifies how often the token bucket is initialized with *burst-size* tokens. *burst-interval* is from 0 to 2147483647 milliseconds (msec).

The *burst-size* is the number of ICMPv6 error messages that can be sent during one *burst-interval*. The range is from 1 to 200 messages.

To disable ICMP rate limiting, set *burst-interval* to zero (0).

Default
- *burst-interval* of 1000 msec.
- *burst-size* of 100 messages

Format `ipv6 icmp error-interval` *burst-interval* [*burst-size*]

Mode Global Config

no ipv6 icmp error-interval

Use the **no** form of the command to return *burst-interval* and *burst-size* to their default values.

Format `no ipv6 icmp error-interval`

Mode Global Config

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

Term	*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.
IPv6 Hop Limit	Shows the unicast hop count used in IPv6 packets originated by the node. For more information, see "ipv6 hop-limit" on page 497.
ICMPv6 Rate Limit Error Interval	Shows how often the token bucket is initialized with burst-size tokens. For more information, see "ipv6 icmp error-interval" on page 506.
ICMPv6 Rate Limit Burst Size	Shows the number of ICMPv6 error messages that can be sent during one *burst-interval.* For more information, see "ipv6 icmp error-interval" on page 506.
Maximum Routes	Shows the maximum IPv6 route table size.

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

```
(Switch) #show ipv6 brief

IPv6 Forwarding Mode.......................... Enable
IPv6 Unicast Routing Mode..................... Enable
IPv6 Hop Limit................................ 0
ICMPv6 Rate Limit Error Interval.............. 1000 msec
ICMPv6 Rate Limit Burst Size.................. 100 messages
Maximum Routes................................ 3000
```

show ipv6 interface

Use this command to show the usability status of IPv6 interfaces and whether ICMPv6 Destination Unreachable messages may be sent.

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:

Term	*Definition*
Interface	The interface in slot/port format.
IPv6 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.

Term	*Definition*
Routing Mode	Shows whether IPv6 routing is enabled or disabled.
IPv6 Enable Mode	Shows whether IPv6 is enabled on the interface.
Administrative Mode	Shows whether the interface administrative mode is enabled or disabled.
Bandwidth	Shows bandwidth of the interface.
Interface Maximum Transmission Unit	The MTU size, in bytes.
Router Duplicate Address Detection Transmits	The number of consecutive duplicate address detection probes to transmit.
Address Autoconfigure Mode	Shows whether the autoconfigure mode is enabled or disabled.
Address DHCP Mode	Shows whether the DHCPv6 client is enabled on the interface.
Router Advertisement NS Interval	The interval, in milliseconds, between router advertisements for advertised neighbor solicitations.
Router Advertisement Lifetime	Shows the router lifetime value of the interface in router advertisements.
Router Advertisement Reachable Time	The amount of time, in milliseconds, to consider a neighbor reachable after neighbor discovery confirmation.
Router Advertisement Interval	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).

Term	*Definition*
IPv6 Destination Unreachables	Shows whether ICMPv6 Destination Unreachable messages may be sent (enabled) or not (disabled). For more information, see "ipv6 unreachables" on page 506.
IPv6 Default Router	Shows the IPv6 address of the default router.

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

```
(Switch) #show ipv6 interface 1/0/1

Routing Mode..................................... Disabled
Administrative Mode.............................. Enabled
IPv6 Operational Mode............................ Disabled
Bandwidth........................................ 100000  kbps
Interface Maximum Transmit Unit.................. 1500
Router Duplicate Address Detection Transmits... 1
Address Autoconfigure Mode.....................Disabled
Address DHCP Mode..............................Enabled
Router Advertisement NS Interval................ 0
Router Advertisement Lifetime.................. 1800
Router Advertisement Reachable Time............ 0
Router Advertisement Interval.................. 600
Router Advertisement Managed Config Flag....... Disabled
Router Advertisement Other Config Flag......... Disabled
Router Advertisement Suppress Flag............. Disabled
IPv6 Destination Unreachables.................. Enabled
IPv6 Default Router............................ fe80::213:c4ff:fedb:6c42

No IPv6 prefixes configured.
```

If an IPv6 prefix is configured on the interface, the following information also appears.

Term	*Definition*
IFPv6 Prefix is	The IPv6 prefix for the specified interface.
Preferred Lifetime	The amount of time the advertised prefix is a preferred prefix.
Valid Lifetime	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 dhcp interface

This command displays a list of all IPv6 addresses currently leased from a DHCP server on a specific in-band interface.

Format `show ipv6 dhcp [interface slot/port]`

Modes Privileged EXEC

Term	*Definition*
Mode	Displays whether the specified interface is in Client mode or not.
State	State of the DHCPv6 Client on this interface.The valid values are: INACTIVE, SOLICIT, REQUEST, ACTIVE, RENEW, REBIND, RELEASE.
Server DUID	DHCPv6 Unique Identifier of the DHCPv6 Server on this interface.
T1 Time	The T1 time specified by the DHCPv6 server. After the client has held the address for this length of time, the client tries to renew the lease.
T2 Time	The T2 time specified by the DHCPv6 server. If the lease renewal fails, then when the client has held the lease for this length of time, the client sends a Rebind message to the server.
Interface IAID	An identifier for an identity association chosen by this client.
Leased Address	The IPv6 address leased by the DHCPv6 Server for this interface.
Preferred Lifetime	The preferred lifetime of the IPv6 address, as defined in RFC 2462.
Valid Lifetime	The valid lifetime of the IPv6 address, as defined by RFC 2462.
Renew Time	The time until the client tries to renew the lease
Expiry Time	The time until the address expires.

show ipv6 neighbor

Use this command to display information about the IPv6 neighbors.

Format `show ipv6 neighbor`

Mode Privileged EXEC

Term	*Definition*
Interface	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.

Term	*Definition*
Neighbor State	State of neighbor cache entry. Possible values are Incomplete, Reachable, Stale, Delay, Probe, and Unknown.
Last Updated	The time in seconds that has elapsed since an entry was added to the cache.

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` keyword 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

Term	*Definition*
Route Codes	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:

Term	*Definition*
Code	The code for the routing protocol that created this routing entry.

Term	*Definition*
Default Gateway	The IPv6 address of the default gateway. When the system does not have a more specific route to a packet's destination, it sends the packet to the default gateway.
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.
Tag	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.
Route-Timestamp	The last updated time for dynamic routes. The format of Route-Timestamp will be • Days:Hours:Minutes if days > = 1 • Hours:Minutes:Seconds if days < 1
Interface	The outgoing router interface to use when forwarding traffic to the next destination. For reject routes, the next hop interface would be `Null0` interface.

To administratively control the traffic destined to a particular network and prevent it from being forwarded through the router, you can configure a static reject route on the router. Such traffic would be discarded and the ICMP destination unreachable message is sent back to the source. This is typically used for preventing routing loops. The reject route added in the RTO is of the type **OSPF Inter-Area**. Reject routes (routes of REJECT type installed by any protocol) are not redistributed by OSPF/RIP. Reject routes are supported in both OSPFv2 and OSPFv3.

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

```
(Routing) #show ipv6 route

IPv6 Routing Table - 3 entries

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

S    2001::/64 [10/0] directly connected,   Null0
C    2003::/64 [0/0]
      via ::,   0/11
S    2005::/64 [1/0]
      via 2003::2,   0/11
C 5001::/64 [0/0]
     via ::,   0/5
OE1 6001::/64 [110/1]
     via fe80::200:42ff:fe7d:2f19,   00h:00m:23s,  0/5
OI 7000::/64 [110/6]
     via fe80::200:4fff:fe35:c8bb,   00h:01m:47s,  0/11
```

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

Term	*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 External	Preference of OSPF external routes.

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

Term	*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.
Reject Routes	Total number of reject routes installed by all protocols.
Number of Prefixes	Summarizes the number of routes with prefixes of different lengths.
Total Routes	The total number of routes in the routing table.

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

```
(Routing) #show ipv6 route summary

IPv6 Routing Table Summary - 3 entries
Connected Routes.............................1
Static Routes................................2
OSPF Routes..................................0
  Intra Area Routes..........................0
  Inter Area Routes..........................0
  External Type-1 Routes.....................0
```

```
  External Type-2 Routes.....................0
Reject Routes..............................1
Total routes...............................3

  Number of Prefixes:
    /64: 3
```

show ipv6 vlan

This command displays IPv6 VLAN routing interface addresses.

Format `show ipv6 vlan`

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
MAC Address used by Routing VLANs	Shows the MAC address.

The rest of the output for this command is displayed in a table with the following column headings:

Column Headings	*Definition*
VLAN ID	The VLAN ID of a configured VLAN.
Logical Interface	The interface in slot/port format that is associated with the VLAN ID.
IPv6 Address/ Prefix Length	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

Term	*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.

Term	*Definition*
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.
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). For entities 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.
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.

Term	*Definition*
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.
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.

Term	*Definition*
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.
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.
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[a]	Number of ICMPv6 Group Membership Response messages sent.
ICMPv6 Group Membership Reduction Messages Received[b]	Number of ICMPv6 Group Membership Reduction messages sent.
ICMPv6 Duplicate Address Detects	Number of duplicate addresses detected by the interface.

a. ICMPv6 Group Membership Response Messages are supported in VxWorks but are not supported in Linux.
b. ICMPv6 Group Membership Reduction Messages are not supported in Linux but are supported in VxWorks.

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. This section includes the following subsections:

Global OSPF Commands

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 area ID 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

no area nssa default-info-originate (OSPFv3)

This command disables the default route advertised into the NSSA.

Format `no 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

no area nssa no-redistribute (OSPFv3)

This command disables the NSSA ABR so that learned external routes are redistributed to the NSSA.

Format `no 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

no area nssa no-summary (OSPFv3)

This command disables nssa from the summary LSAs.

Format `no 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

no area nssa translator-role (OSPFv3)

This command disables the nssa translator role from the specified area id.

Format `no 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

no area nssa translator-stab-intv (OSPFv3)

This command disables the nssa translator's *stabilityinterval* from the specified area id.

Format `no 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 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.

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

auto-cost (OSPFv3)

By default, OSPF computes the link cost of each interface from the interface bandwidth. Faster links have lower metrics, making them more attractive in route selection. The configuration parameters in the `auto-cost reference bandwidth` and `bandwidth` commands give you control over the default link cost. You can configure for OSPF an interface bandwidth that is independent of the actual link speed. A second configuration parameter allows you to control the ratio of interface bandwidth to link cost. The link cost is computed as the ratio of a reference bandwidth to the interface bandwidth (ref_bw / interface bandwidth), where interface bandwidth is defined by the `bandwidth` command. Because the default reference bandwidth is 100 Mbps, OSPF uses the same default link cost for all interfaces whose bandwidth is 100 Mbps or greater. Use the `auto-cost` command to change the reference bandwidth, specifying the reference bandwidth in megabits per second (Mbps). The reference bandwidth range is 1–4294967 Mbps.

Default 100Mbps

Format `auto-cost reference-bandwidth 1-4294967`

Mode Router OSPFv3 Config

no auto-cost reference-bandwidth (OSPFv3)

Use this command to set the reference bandwidth to the default value.

Format `no auto-cost reference-bandwidth`

Mode Router OSPFv3 Config

clear ipv6 ospf

Use this command to disable and re-enable OSPF.

Format `clear ipv6 ospf`

Mode Privileged EXEC

clear ipv6 ospf configuration

Use this command to reset the OSPF configuration to factory defaults.

Format `clear ipv6 ospf configuration`

Mode Privileged EXEC

clear ipv6 ospf counters

Use this command to reset global and interface statistics.

Format `clear ipv6 ospf counters`

Mode Privileged EXEC

clear ipv6 ospf neighbor

Use this command to drop the adjacency with all OSPF neighbors. On each neighbor's interface, send a one-way hello. Adjacencies may then be re-established. To drop all adjacencies with a specific router ID, specify the neighbor's Router ID using the optional parameter [*neighbor-id*].

Format `clear ipv6 ospf neighbor` *`[neighbor-id]`*

Mode Privileged EXEC

clear ipv6 ospf neighbor interface

To drop adjacency with all neighbors on a specific interface, use the optional parameter [slot/port]. To drop adjacency with a specific router ID on a specific interface, use the optional parameter [*neighbor-id*].

Format `clear ipv6 ospf neighbor interface` *`[slot/port] [neighbor-id]`*

Mode Privileged EXEC

clear ipv6 ospf redistribution

Use this command to flush all self-originated external LSAs. Reapply the redistribution configuration and re-originate prefixes as necessary.

Format `clear ipv6 ospf redistribution`

Mode Privileged EXEC

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 route types in the router. Lower route preference values are preferred when determining the best route. The type of OSPF route can be intra, inter, or external. All the external type routes are given the same preference value. The range of *preference* value is 1 to 255.

Default 110

Format `distance ospf {intra-area 1-255 | inter-area 1-255 | external 1-255}`

Mode Router OSPFv3 Config

no distance ospf

This command sets the default route preference value of OSPF routes in the router. The type of OSPF route can be intra, inter, or external. All the external type routes are given the same preference value.

Format `no distance ospf {intra-area | inter-area | external}`

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

passive-interface default (OSPFv3)

Use this command to enable global passive mode by default for all interfaces. It overrides any interface level passive mode. OSPF shall not form adjacencies over a passive interface.

Default disabled

Format `passive-interface default`

Mode Router OSPFv3 Config

no passive-interface default

Use this command to disable the global passive mode by default for all interfaces. Any interface previously configured to be passive reverts to non-passive mode.

Format `no passive-interface default`

Mode Router OSPFv3 Config

passive-interface (OSPFv3)

Use this command to set the interface or tunnel as passive. It overrides the global passive mode that is currently effective on the interface or tunnel.

Default disabled

Format `passive-interface {slot/port | tunnel` *`tunnel-id`*`}`

Mode Router OSPFv3 Config

no passive-interface

Use this command to set the interface or tunnel as non-passive. It overrides the global passive mode that is currently effective on the interface or tunnel.

Format `no passive-interface {slot/port | tunnel` *`tunnel-id`*`}`

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 (OSPFv3)

Use this command to enable individual OSPF traps, enable a group of trap flags at a time, or enable all the trap flags at a time. The different groups of trapflags, and each group's specific trapflags to enable or disable, are listed in Table 13.

Table 13: Trapflag Groups (OSPFv3)

Group	*Flags*
errors	• authentication-failure • bad-packet • config-error • virt-authentication-failure • virt-bad-packet • virt-config-error
if-rx	ir-rx-packet
lsa	• lsa-maxage • lsa-originate
overflow	• lsdb-overflow • lsdb-approaching-overflow
retransmit	• packets • virt-packets
rtb	• rtb-entry-info
state-change	• if-state-change • neighbor-state-change • virtif-state-change • virtneighbor-state-change

- To enable the individual flag, enter the `group name` followed by that particular flag.
- To enable all the flags in that group, give the group name followed by `all`.
- To enable all the flags, give the command as `trapflags all`.

Default disabled

Format

```
trapflags {
all |
errors {all | authentication-failure | bad-packet | config-error | virt-
authentication-failure | virt-bad-packet | virt-config-error} |
if-rx {all | if-rx-packet} |
lsa {all | lsa-maxage | lsa-originate} |
overflow {all | lsdb-overflow | lsdb-approaching-overflow} |
retransmit {all | packets | virt-packets} |
rtb {all, rtb-entry-info} |
state-change {all | if-state-change | neighbor-state-change | virtif-state-change |
virtneighbor-state-change}
}
```

Mode Router OSPFv3 Config

no trapflags

Use this command to revert to the default reference bandwidth.

- To disable the individual flag, enter the `group name` followed by that particular flag.
- To disable all the flags in that group, give the group name followed by `all`.
- To disable all the flags, give the command as `trapflags all`.

Format
```
no trapflags {
all |
errors {all | authentication-failure | bad-packet | config-error | virt-
authentication-failure | virt-bad-packet | virt-config-error} |
if-rx {all | if-rx-packet} |
lsa {all | lsa-maxage | lsa-originate} |
overflow {all | lsdb-overflow | lsdb-approaching-overflow} |
retransmit {all | packets | virt-packets} |
rtb {all, rtb-entry-info} |
state-change {all | if-state-change | neighbor-state-change | virtif-state-
change | virtneighbor-state-change}
}
```

Mode Router OSPFv3 Config

OSPFv3 Interface Commands

ipv6 ospf area

This command sets the OSPF area to which the specified router interface or range of interfaces belongs. It also enables OSPF on the specified router interface or range of interfaces. The *area* is a 32-bit integer, formatted as a 4-digit dotted-decimal number or a decimal value in the range of 0–4294967295. The *area* uniquely identifies the area to which the interface connects. Assigning an area ID for an area that does not yet exist, causes the area to be created with default values.

Format `ipv6 ospf area` *0-4294967295*

Mode Interface Config

ipv6 ospf cost

This command configures the cost on an OSPF interface or range of interfaces. 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 or range of interfaces. 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 1-2147483647`

Mode Interface Config

no ipv6 ospf dead-interval

This command sets the default OSPF dead interval for the specified interface or range of interfaces.

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 on an interface or range of interfaces. 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 or range of interfaces. 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 `no ipv6 ospf network {broadcast | point-to-point}`

Mode Interface Config

ipv6 ospf priority

This command sets the OSPF priority for the specified router interface or range of interfaces. 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 or range of interfaces. 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 or range of interfaces. 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

OSPFv3 Graceful Restart Commands

The OSPFv3 protocol can be configured to participate in the checkpointing service, so that these protocols can execute a *graceful restart* when the management unit fails. In a graceful restart, the hardware to continues forwarding IPv6 packets using OSPFv3 routes while a backup switch takes over management unit responsibility

Graceful restart uses the concept of *helpful neighbors*. A fully adjacent router enters helper mode when it receives a link state announcement (LSA) from the restarting management unit indicating its intention of performing a graceful restart. In helper mode, a switch continues to advertise to the rest of the network that they have full adjacencies with the restarting router, thereby avoiding announcement of a topology change and and the potential for flooding of LSAs and shortest-path-first (SPF) runs (which determine OSPF routes). Helpful neighbors continue to forward packets through the restarting router. The restarting router relearns the network topology from its helpful neighbors.

Graceful restart can be enabled for either planned or unplanned restarts, or both. A planned restart is initiated by the operator through the management command `initiate failover`. The operator may initiate a failover in order to take the management unit out of service (for example, to address a partial hardware failure), to correct faulty system behavior which cannot be corrected through less severe management actions, or other reasons. An unplanned restart is an unexpected failover caused by a fatal hardware failure of the management unit or a software hang or crash on the management unit.

nsf (OSPFv3)

Use this command to enable the OSPF graceful restart functionality on an interface. To disable graceful restart, use the no form of the command.

Default Disabled

Format `nsf [ietf] [planned-only]`

Modes Router OSPFv3 Config

Parameter	*Description*
ietf	This keyword is accepted but not required.
planned-only	This optional keyword indicates that OSPF should only perform a graceful restart when the restart is planned (i.e., when the restart is a result of the initiate failover command).

no nsf (OSPFv3)

Use this command to disable graceful restart for all restarts.

nsf restart-interval (OSPFv3)

Use this command to configure the number of seconds that the restarting router asks its neighbors to wait before exiting helper mode. This is referred to as the grace period. The restarting router includes the grace period in its grace LSAs. For planned restarts (using the `initiate failover` command), the grace LSAs are sent prior to restarting the management unit, whereas for unplanned restarts, they are sent after reboot begins.

The grace period must be set long enough to allow the restarting router to reestablish all of its adjacencies and complete a full database exchange with each of those neighbors.

Default 120 seconds

Format `nsf [ietf] restart-interval` *`1-1800`*

Modes Router OSPFv3 Config

Parameter	*Description*
ietf	This keyword is accepted but not required.
seconds	The number of seconds that the restarting router asks its neighbors to wait before exiting helper mode. The range is from 1 to 1800 seconds.

no nsfrestart-interval (OSPFv3)

Use this command to revert the grace period to its default value.

Format `no [ietf] nsf restart-interval`

Modes Router OSPFv3 Config

nsf helper (OSPFv3)

Use this command to enable helpful neighbor functionality for the OSPF protocol. You can enable this functionality for planned or unplanned restarts, or both.

Default OSPF may act as a helpful neighbor for both planned and unplanned restarts

Format `nsf helper [planned-only]`

Modes Router OSPFv3 Config

Parameter	*Description*
planned-only	This optional keyword indicates that OSPF should only help a restarting router performing a planned restart.

no nsf helper (OSPFv3)

Use this command to disable helpful neighbor functionality for OSPF.

Format `no nsf helper`

Modes Router OSPFv3 Config

nsf ietf helper disable (OSPFv3)

Use this command to disable helpful neighbor functionality for OSPF.

Note: The commands `no nsf helper` and `nsf ietf helper disable` are functionally equivalent. The command `nsf ietf helper disable` is supported solely for compatibility with other network software CLI.

Format `nsf ietf helper disable`

Modes Router OSPFv3 Config

nsf helper strict-lsa-checking (OSPFv3)

The restarting router is unable to react to topology changes. In particular, the restarting router will not immediately update its forwarding table; therefore, a topology change may introduce forwarding loops or black holes that persist until the graceful restart completes. By exiting the graceful restart on a topology change, a router tries to eliminate the loops or black holes as quickly as possible by routing around the restarting router. A helpful neighbor considers a link down with the restarting router to be a topology change, regardless of the strict LSA checking configuration.

Use this command to require that an OSPF helpful neighbor exit helper mode whenever a topology change occurs.

Default Enabled.

Format `nsf [ietf] helper strict-lsa-checking`

Modes Router OSPFv3 Config

Parameter	*Description*
ietf	This keyword is accepted but not required.

no nsf [ietf] helper strict-lsa-checking (OSPFv3)

Use this command to allow OSPF to continue as a helpful neighbor in spite of topology changes.

Default Enabled.

Format `nsf [ietf] helper strict-lsa-checking`

Modes Router OSPFv3 Config

OSPFv3 Show Commands

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.

Term	*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.
External LSDB Limit	The maximum number of non-default AS-external-LSAs entries that can be stored in the link-state database.
Exit Overflow Interval	The number of seconds that, after entering overflow state, a router will attempt to leave overflow state.
AutoCost Ref BW	Shows the value of the auto-cost reference bandwidth configured on the router.
Default Passive Setting	Shows whether the interfaces are passive by default.
Maximum Paths	The maximum number of paths that OSPF can report for a given destination.
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	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.
Number of Active Areas	The number of active OSPF areas. An *active* OSPF area is an area with at least one interface up.
ABR Status	Shows whether the router is an OSPF Area Border Router.
ASBR Status	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 learned by other protocols) or disabled (if the router is not configured for the same).

Term	*Definition*
Stub Router	When OSPF runs out of resources to store the entire link state database, or any other state information, OSPF goes into stub router mode. As a stub router, OSPF re-originates its own router LSAs, setting the cost of all non-stub interfaces to infinity. To restore OSPF to normal operation, disable and re-enable OSPF.
External LSDB Overflow	When the number of non-default external LSAs exceeds the configured limit, External LSDB Limit, OSPF goes into LSDB overflow state. In this state, OSPF withdraws all of its self-originated non-default external LSAs. After the Exit Overflow Interval, OSPF leaves the overflow state, if the number of external LSAs has been reduced.
External LSA Count	The number of external (LS type 5) link-state advertisements in the link-state database.
External LSA Checksum	The sum of the LS checksums of external link-state advertisements contained in the link-state database.
New LSAs Originated	The number of new link-state advertisements that have been originated.
LSAs Received	The number of link-state advertisements received determined to be new instantiations.
LSA Count	The total number of link state advertisements currently in the link state database.
Maximum Number of LSAs	The maximum number of LSAs that OSPF can store.
LSA High Water Mark	The maximum size of the link state database since the system started.
Retransmit List Entries	The total number of LSAs waiting to be acknowledged by all neighbors. An LSA may be pending acknowledgment from more than one neighbor.
Maximum Number of Retransmit Entries	The maximum number of LSAs that can be waiting for acknowledgment at any given time.
Retransmit Entries High Water Mark	The highest number of LSAs that have been waiting for acknowledgment.
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	The metric of the routes being redistributed.
Metric Type	Shows whether the routes are External Type 1 or External Type 2.
Tag	The decimal value attached to each external route.
Subnets	For redistributing routes into OSPF, the scope of redistribution for the specified protocol.
Distribute-List	The access list used to filter redistributed routes.
NSF Support	Indicates whether nonstop forwarding (NSF) is enabled for the OSPF protocol for planned restarts, unplanned restarts or both (Always).
NSF Restart Interval	The user-configurable grace period during which a neighboring router will be in the helper state after receiving notice that the management unit is performing a graceful restart.
NSF Restart Status	The current graceful restart status of the router.
NSF Restart Age	Number of seconds until the graceful restart grace period expires.

Term	*Definition*
NSF Restart Exit Reason	Indicates why the router last exited the last restart: • None — Graceful restart has not been attempted. • In Progress — Restart is in progress. • Completed — The previous graceful restart completed successfully. • Timed Out — The previous graceful restart timed out. • Topology Changed — The previous graceful restart terminated prematurely because of a topology change.
NSF Help Support	Indicates whether helpful neighbor functionality has been enabled for OSPF for planned restarts, unplanned restarts, or both (Always).
NSF help Strict LSA checking	Indicates whether strict LSA checking has been enabled. If enabled, then an OSPF helpful neighbor will exit helper mode whenever a topology change occurs. If disabled, an OSPF neighbor will continue as a helpful neighbor in spite of topology changes.

show ipv6 ospf abr

This command displays the internal OSPFv3 routes to reach Area Border Routers (ABR). This command takes no options.

Format `show ipv6 ospf abr`

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
Type	The type of the route to the destination. It can be either: • 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.
Next Hop	Next hop toward the destination.
Next Hop Intf	The outgoing router interface to use when forwarding traffic to the next hop.

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

Term	*Definition*
AreaID	The area id of the requested OSPF area.
External Routing	A number representing the external routing capabilities for this area.
Spf Runs	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.
Import Summary LSAs	Shows whether to import summary LSAs (enabled).
OSPF Stub Metric Value	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.

Term	*Definition*
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	The metric value for the default route advertised into the NSSA.
Default Metric Type	The metric type for the default route advertised into the NSSA.
Translator Role	The NSSA translator role of the ABR, which is always or candidate.
Translator Stability Interval	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 asbr

This command displays the internal OSPFv3 routes to reach Autonomous System Boundary Routers (ASBR). This command takes no options.

Format `show ipv6 ospf asbr`

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
Type	The type of the route to the destination. It can be either: • 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.
Next Hop	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 | net work | 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.

Term	*Definition*
Link Id	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	A number representing the age of the link state advertisement in seconds.
Sequence	A number that represents which LSA is more recent.
Checksum	The total number LSA checksum.
Options	An integer indicating 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

Term	*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

Term	*Definition*
IP Address	The IPv6 address of the interface.
ifIndex	The interface index number associated with the interface.
OSPF Admin Mode	Shows whether the admin mode is enabled or disabled.
OSPF Area ID	The area ID associated with this interface.
Router Priority	The router priority. The router priority determines which router is the designated router.
Retransmit Interval	The frequency, in seconds, at which the interface sends LSA.
Hello Interval	The frequency, in seconds, at which the interface sends Hello packets.
Dead Interval	The amount of time, in seconds, the interface waits before assuming a neighbor is down.
LSA Ack Interval	The amount of time, in seconds, the interface waits before sending an LSA acknowledgement after receiving an LSA.
Interface Transmit Delay	The number of seconds the interface adds to the age of LSA packets before transmission.
Authentication Type	The type of authentication the interface performs on LSAs it receives.
Metric Cost	The priority of the path. Low costs have a higher priority than high costs.
Passive Status	Shows whether the interface is passive or not.
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:

Term	*Definition*
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 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

Term	*Definition*
Interface	*slot/port*
OSPF Admin Mode	States whether OSPF is enabled or disabled on a router interface.
OSPF Area ID	The OSPF Area ID for the specified interface.
Router Priority	The router priority. The router priority determines which router is the designated router.
Metric Cost	The priority of the path. Low costs have a higher priority than high costs.
Hello Interval	The frequency, in seconds, at which the interface sends Hello packets.
Dead Interval	The amount of time, in seconds, the interface waits before assuming a neighbor is down.
Retransmit Interval	The frequency, in seconds, at which the interface sends LSA.
Retransmit Delay Interval	The number of seconds the interface adds to the age of LSA packets before transmission.
LSA Ack Interval	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 displays information only if OSPF is enabled.

Format `show ipv6 ospf interface stats slot/port`

Modes
- Privileged EXEC
- User EXEC

Term	*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.

Term	*Definition*
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.
Sent Packets	The number of OSPF packets transmitted on the interface.
Received Packets	The number of valid OSPF packets received on the interface.
Discards	The number of received OSPF packets discarded because of an error in the packet or an error in processing the packet.
Bad Version	The number of received OSPF packets whose version field in the OSPF header does not match the version of the OSPF process handling the packet.
Virtual Link Not Found	The number of received OSPF packets discarded where the ingress interface is in a non-backbone area and the OSPF header identifies the packet as belonging to the backbone, but OSPF does not have a virtual link to the packet's sender.
Area Mismatch	The number of OSPF packets discarded because the area ID in the OSPF header is not the area ID configured on the ingress interface.
Invalid Destination Address	The number of OSPF packets discarded because the packet's destination IP address is not the address of the ingress interface and is not the AllDrRouters or AllSpfRouters multicast addresses.
No Neighbor at Source Address	The number of OSPF packets dropped because the sender is not an existing neighbor or the sender's IP address does not match the previously recorded IP address for that neighbor. NOTE: Does not apply to Hellos.
Invalid OSPF Packet Type	The number of OSPF packets discarded because the packet type field in the OSPF header is not a known type.
Hellos Ignored	The number of received Hello packets that were ignored by this router from the new neighbors after the limit has been reached for the number of neighbors on an interface or on the system as a whole.

Table 11 on page 453 lists the number of OSPF packets of each type sent and received on the 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:

Term	*Definition*
Router ID	The 4-digit dotted-decimal number of the neighbor router.
Priority	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	The interface ID of the neighbor.
Interface	The interface of the local router in slot/port format.
State	The state of the neighboring routers. Possible values are: • 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. • Full - the neighboring routers are fully adjacent and they will now appear in router-LSAs and network-LSAs.
Dead Time	The amount of time, in seconds, to wait before the router assumes the neighbor is unreachable.
Restart Helper Status	Indicates the status of this router as a helper during a graceful restart of the router specified in the command line: • Helping—This router is acting as a helpful neighbor to the specified router. • Not Helping—This router is not a helpful neighbor at this time.
Restart Reason	When this router is in helpful neighbor mode, this indicates the reason for the restart as provided by the restarting router.
Remaining Grace Time	The number of seconds remaining the in current graceful restart interval. This is displayed only when this router is currently acting as a helpful neighbor for the router specified in the command.
Restart Helper Exit Reason	Indicates the reason that the specified router last exited a graceful restart. • None—Graceful restart has not been attempted • In Progress—Restart is in progress • Completed—The previous graceful restart completed successfully • Timed Out—The previous graceful restart timed out • Topology Changed—The previous graceful restart terminated prematurely because of a topology change

If you specify an IP address for the neighbor router, the following fields display:

Term	*Definition*
Interface	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	The router priority for the specified interface.
Dead Timer Due	The amount of time, in seconds, to wait before the router assumes the neighbor is unreachable.
State	The state of the neighboring routers.
Events	Number of times this neighbor relationship has changed state, or an error has occurred.
Retransmission Queue Length	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 area ID. The *areaid* identifies the OSPF area whose ranges are being displayed.

Format `show ipv6 ospf range areaid`

Modes
- Privileged EXEC
- User EXEC

Term	*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

Term	*Definition*
Area ID	A 32-bit identifier for the created stub area.
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

Term	*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.
Interface Transmit Delay	The configured transmit delay for the OSPF virtual interface.
Retransmit Interval	The configured retransmit interval for the OSPF virtual interface.
Authentication Type	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`

Modes
- Privileged EXEC
- User EXEC

Term	*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.
Transmit Delay	The configured transmit delay for the OSPFV3 virtual interface.

DHCPv6 Commands

This section describes the commands 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 or range of interfaces. 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 on an interface or range of interfaces. 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 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.

no domain-name

Format `domain-name dns-domain-name`

Mode IPv6 DHCP Pool Config

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
- valid-lifetime—2592000
- preferred-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

Term	*Definition*
DHCPv6 is Enabled (Disabled)	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

Term	*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.
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

Term	*Definition*
IPv6 Interface	The interface name in slot/port format.
Mode	Shows whether the interface is a IPv6 DHCP relay or server.

If the interface mode is server, the following information displays.

Term	*Definition*
Pool Name	The pool name specifying information for DHCPv6 server distribution to DHCPv6 clients.
Server Preference	The preference of the server.
Option Flags	Shows whether rapid commit is enabled.

If the interface mode is relay, the following information displays.

Term	*Definition*
Relay Address	The IPv6 address of the relay server.
Relay Interface Number	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 556 for information about the output.

show ipv6 dhcp pool

This command displays configured DHCP pool.

Format `show ipv6 dhcp pool` *`pool-name`*

Mode Privileged EXEC

Term	*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

Term	*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.

show network ipv6 dhcp statistics

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

Format `show network ipv6 dhcp statistics`

Mode
- Privileged EXEC
- User EXEC

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

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

```
(admin)#show network ipv6 dhcp statistics
DHCPv6 Client Statistics
------------------------

DHCPv6 Advertisement Packets Received..... 0
DHCPv6 Reply Packets Received..... 0
Received DHCPv6 Advertisement Packets Discarded..... 0
Received DHCPv6 Reply Packets Discarded..... 0
DHCPv6 Malformed Packets Received..... 0
Total DHCPv6 Packets Received..... 0

DHCPv6 Solicit Packets Transmitted..... 0
DHCPv6 Request Packets Transmitted..... 0
```

```
DHCPv6 Renew Packets Transmitted..................... 0
DHCPv6 Rebind Packets Transmitted.................... 0
DHCPv6 Release Packets Transmitted................... 0
Total DHCPv6 Packets Transmitted..................... 0
```

show serviceport ipv6 dhcp statistics

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

Format `show serviceport ipv6 dhcp statistics`

Mode
- Privileged EXEC
- User EXEC

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

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

```
(admin)#show serviceport ipv6 dhcp statistics
DHCPv6 Client Statistics
------------------------

DHCPv6 Advertisement Packets Received................ 0
DHCPv6 Reply Packets Received........................ 0
Received DHCPv6 Advertisement Packets Discarded...... 0
```

```
Received DHCPv6 Reply Packets Discarded.............. 0
DHCPv6 Malformed Packets Received.................... 0
Total DHCPv6 Packets Received........................ 0

DHCPv6 Solicit Packets Transmitted................... 0
DHCPv6 Request Packets Transmitted................... 0
DHCPv6 Renew Packets Transmitted..................... 0
DHCPv6 Rebind Packets Transmitted.................... 0
DHCPv6 Release Packets Transmitted................... 0
Total DHCPv6 Packets Transmitted..................... 0
```

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

clear network ipv6 dhcp statistics

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

Format `clear network ipv6 dhcp statistics`

Mode
- Privileged EXEC

clear serviceport ipv6 dhcp statistics

Use this command to clear the DHCPv6 client statistics on the service port interface.

Format `clear serviceport ipv6 dhcp statistics`

Mode
- Privileged EXEC

Section 8: Wireless Commands

This section describes the CLI commands you use to manage the wireless features on the switch as well as the wireless access points that a switch manages.

This section contains the following subsections:

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

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

Wireless Switch Commands

The commands in this section provide global Wireless Switch configuration, status, and statistics.

wireless

This command enters the Wireless Switch global configuration mode.

Format `wireless`

Mode Global Config

enable (Wireless Config Mode)

This command enables the Wireless Switch functionality.

Default Enable

Format `enable`

Mode Wireless Config

no enable

The `no` version of this command disables the Wireless Switch functionality.

Format `no enable`

Mode Wireless Config

country-code

This command globally configures the country code for the Wireless Switch and all managed access points. The code may be entered in either upper or lower case. When you change the country code, the wireless function is disabled and re-enabled automatically. The `show country-code` command displays all valid country codes.

Default US

Format `country-code` *`code`*

Mode Wireless Config

Parameter	*Description*
code	This parameter must identify a valid country code.

Example: The following shows an example of the command.

```
(Switch) (Config wireless)# country-code au <cr>
Are you sure you want to change the country code? (y/n)
```

no country-code

The no version of this command returns the configured country code to the default.

Format no country-code

Mode Wireless Config

OUI database

This command adds a new entry to the OUI database, if not already present. Each entry consists of an OUI Value, which is composed of the higher three octets of the Ethernet MAC address of the AP/Client and the organization name for the OUI, which is a 32-byte string.

Format oui database *ouival oui*

Mode Wireless Config Mode

Parameter	*Description*
ouival	OUI Value of the vendor of AP/Client.
oui	Organization name for the OUI.

Example: The following example adds an OUI entry with the value and vendor name as shown.

```
Switch (Config-wireless)# oui database 00:00:01 "VendorName"
```

no OUI database

The no version of this command deletes the OUI entry for the specified OUI Value from the local OUI database.

Format no oui database *ouival*

Mode Wireless Config Mode

peer-group

This command indicates the peer group for this switch. There may be more than one group of peer switches on the same WLAN. A peer group is created by configuring all peers within the group with the same identifier.

Default 1

Format peer-group {1-255}

Mode Wireless Config

Parameter	*Description*
1–255	The identifier for the peer switch group. The range is from 1 to 255.

no peer-group

The no version of this command returns the configured peer switch group to the default.

Format no peer-group

Mode Wireless Config

discovery method

This command enables various methods used for the discovery of APs and peer switches. If no method is specified, then it enables all the discovery methods.

Default IP-Polling – Enable, L2-Multicast - Enable

Format discovery method [{ip-poll | l2-multicast}]

Mode Wireless Config

Parameter	*Description*
ip-poll	Enable IP-based discovery of APs and peer switches.
l2-multicast	Enable L2-based discovery of APs and peer switches.

no discovery method

The no version of this command disables the specified discovery method. If no method is specified, then it disables all the discovery methods.

Format no discovery method [{ip-poll | l2-multicast}]

Mode Wireless Config

discovery ip-list

This command adds an IP address to the list of addresses global to the Wireless Switch. The switch polls each address in the list to discover new access points and peers. The list is used when discovery via IP polling is enabled.

Format `discovery ip-list ipaddr`

Mode Wireless Config

Parameter	*Description*
ipaddr	A valid IP address.

no discovery ip-list

The no version of this command deletes the specified IP address from the polling list. If an argument is not specified, all entries are deleted from the polling list.

Format `no discovery ip-list [ipaddr]`

Mode Wireless Config

discovery vlan-list

This command adds VLAN IDs on which to send L2 discovery multicast frames. Up to 16 VLAN IDs can be configured. By default, there is one entry in the list, 1 - Default VLAN.

Default 1 – Default VLAN

Format `discovery vlan-list vlan-id`

Mode Wireless Config

Parameter	*Description*
vlan-id	A VLAN ID in the range 1 to 4094.

no discovery vlan-list

The no version of this command deletes the VLAN ID from the discovery list. If no arguments are specified, all VLANs are deleted from the list except for the first entry. At least one entry must be configured in the list.

Format `no discovery vlan-list [vlan-id]`

Mode Wireless Config

l2tunnel vlan-list

This command adds VLAN IDs to the centralized L2 tunneling tunneled VLAN list. Up to 64 VLAN IDs can be configured. By default, there are no entries in this list.

Default None

Format `l2tunnel vlan-list` *`vlan-id`*

Mode Wireless Config

Parameter	*Description*
vlan-id	A VLAN ID in the range 1 to 4094.

no l2tunnel vlan-list

The `no` version of this command deletes the VLAN ID from the tunneled VLAN list. If no arguments are specified, all VLANs are deleted from the list.

Format `no l2tunnel vlan-list` *`vlan-id`*

Mode Wireless Config

ap validation

This command configures whether to use the local valid AP database or a RADIUS server to validate newly discovered APs.

Default local

Format `ap validation {local | radius}`

Mode Wireless Config

Parameter	*Description*
local	Local database is used for validating discovered APs.
radius	RADIUS server is used for validating discovered APs.

ap authentication

This command enables AP authentication. When enabled, all APs are required to authenticate to the Wireless Switch using a password upon discovery.

Default	Disable
Format	`ap authentication`
Mode	Wireless Config

no ap authentication

The `no` version of this command disables AP authentication. APs are not required to authenticate to the Wireless Switch upon discovery.

Format	`no ap authentication`
Mode	Wireless Config

ap auto-upgrade

This command enables AP Auto-Upgrade mode on a wireless switch that supports both the Independent and the Integrated AP image download modes.

Default	Disable
Format	`auto-upgrade`
Mode	Wireless Config

no ap auto-upgrade

The no version of this command disables the AP auto upgrade mode on the wireless switch.

Format	`no ap auto-upgrade`
Mode	Wireless Config

ap client-qos

This command enables AP client QoS operation globally for the wireless switch. When enabled, and when the network client QoS mode is also enabled, clients associated to that network may have one or more of the following QoS characteristics in effect in the down and/or up directions: access control, bandwidth limiting, and differentiated services.

Note: This command takes effect in an AP without requiring that the AP profile be re-applied.

Default Disable

Format `ap client-qos`

Mode Wireless Config

no ap client-qos

The `no` version of this command disables AP client QoS operation globally. Client traffic is not subject to QoS processing in any APs attached to this wireless switch.

Format `no ap client-qos`

Mode Wireless Config

snmp-server enable traps wireless

This command globally enables the Wireless Switch SNMP traps. The specific wireless trap groups are configured using the `trapflags` command in Wireless Config Mode.

Default Disable

Format `snmp-server enable traps wireless`

Mode Global Config

no snmp-server enable traps wireless

The `no` version of this command globally disables all Wireless Switch SNMP traps.

Format `no snmp-server enable traps wireless`

Mode Global Config

trapflags (Wireless Config Mode)

This command enables Wireless Switch SNMP trap groups for wireless system events. If no parameters are specified, then all traps are enabled.

Default All - Disable

Format `trapflags [{ap-failure | ap-state | client-failure | client-state | peer-ws | rf-scan | rogue-ap | tspec | wids-status | ws-status}]`

Mode Wireless Config

Parameter	*Description*
ap-failure	Enable/Disable SNMP traps associated with AP association/authentication failures.
ap-state	Enable/Disable SNMP traps associated with AP state changes.
client-failure	Enable/Disable SNMP traps associated with client association/authentication failures.
client-state	Enable/Disable SNMP traps associated with client state changes.
peer-ws	Enable/Disable SNMP traps associated with peer Wireless Switch events.
rf-scan	Enable/Disable SNMP traps associated with RF scan related events.
rogue-ap	Enable/Disable SNMP traps associated with rogue access points.
tspec	Enable/Disable SNMP traps associated with TSPEC events.
wids-status	Enable/Disable SNMP traps associated with WIDS status events.
ws-status	Enable/Disable SNMP traps associated with wireless status events.

no trapflags

The no version of this command disables Wireless Switch SNMP trap groups for wireless system events. If no parameters are specified, then all traps are disabled.

Format `no trapflags [{ap-failure | ap-state | client-failure | client-state | peer-ws | rf-scan | rogue-ap | tspec | wids-status | ws-status}]`

Mode Wireless Config

agetime

This command configures database entry age times for the Wireless Switch. A time value of 0 indicates entries in the corresponding database will not age and you must manually delete them.

Default 24 hours

Format `agetime {ad-hoc | ap-failure | client-failure | rf-scan |detected-client} <0,1-168>`

Mode Wireless Config

Parameter	*Description*
ad-hoc	Time in hours to maintain an entry in the ad hoc client network list.
ap-failure	Time in hours to maintain an entry in the AP association and authentication failure list.
client-failure	Time in hours to maintain an entry in the client association and authentication failure list.
rf-scan	Time in hours to maintain an entry obtained from an RF scan.
detected-client	Time in hours to maintain an entry in the detected clients database.
0,1–168	Time in hours from 0 to 168. A value of 0 indicates that entries should never age out.

no agetime

The `no` version of this command returns the configured entry age time to the default.

Format `no agetime {ad-hoc | ap-failure | client-failure | rf-scan |detected-client}`

Mode Wireless Config

peer-switch configuration

This command enables peer switch configuration for the wireless system. When a group is enabled, the corresponding configuration is applied to one or more peer switches during a peer switch configuration request. If no parameters are specified, then all switch configuration groups are enabled.

Default

- ap-database - Enable
- ap-profile - Enable,
- captive-portal - Enable
- channel-power - Enable,
- discovery – Disable,
- global – Enable,
- known-client – Enable
- radius-client – Enable

Format `peer-switch configuration [{ap-database|ap-profile|captive-portal|channel-power|discovery|global|known-client|radius-client}]`

Mode Wireless Config

Parameter	*Description*
ap-database	Enable/Disable AP database configuration push to peer switches.
ap-profile	Enable/Disable AP profile and network configuration push to peer switches.
captive-portal	Enable/Disable Captive Portal configuration push to peer switches.
channel-power	Enable/Disable channel and power configuration push to peer switches.
discovery	Enable/Disable discovery configuration push to peer switches.
global	Enable/Disable global configuration push to peer switches.
known-client	Enable/Disable known client database push to peer switches.
radius-client	Enable/Disable RADIUS client configuration push to peer switches.

no peer-switch configuration

The no version of this command disables peer switch configuration for the wireless system. If no parameters are specified, then all peer switch configurations are disabled.

Format `no peer-switch configuration [{ap-database|ap-profile|captive-portal| channel-power|discovery|global|known-client|radius-client}]`

Mode Wireless Config

tspec violation-interval

This command configures the TSPEC client violation report interval, in seconds, for the wireless switch. This interval is the time period at which wireless clients detected as using admission-controlled resources without proper TSPEC authorization are reported via the system logging facility and SNMP trap mechanisms. A time value of 0 disables this reporting.

Default `300 seconds`

Format `tspec violation-interval` *`seconds`*

Mode Wireless Config

Parameter	*Description*
seconds	Time in seconds from 0 to 900. A value of 0 indicates that violating clients are not reported.

no tspec violation-interval

The no version of this command returns the configured entry age time to the default value.

Format `no tspec violation-interval`

Mode Wireless Config

wireless peer-switch configure

This command allows the administrator to initiate a configuration push to one or all peer switches. If no parameters are given, all peer switches are configured. If the optional IP address parameter is specified, only that peer switch is configured.

Format `wireless peer-switch configure [ipaddr]`

Mode Privileged EXEC

Parameter	*Description*
ipaddr	Peer switch IP address.

wireless rrm channel-load request abort

This command pertains to the Radio Resource Measurement (RRM) capabilities as described in the IEEE 802.11k specification.This command aborts a pending measurement request to a wireless client. This command must be executed from the cluster controller.

Format `wireless rrm channel-load request abort`

Mode Privileged EXEC

wireless rrm channel-load request channel

This command pertains to the Radio Resource Measurement (RRM) capabilities as described in the IEEE 802.11k specification. It allows the administrator to set the channel to use in the next channel load measurement request. A channel value may be supplied, or `all` may be used to indicate to the wireless client in question that the next channel load measurement should occur on all supported channels. This command must be executed from the cluster controller.

Format `wireless rrm channel-load request channel [channel | all]`

Mode Privileged EXEC

Parameter	*Description*
channel	A specific wireless channel.

wireless rrm channel-load request client

This command pertains to the Radio Resource Measurement (RRM) capabilities as described in the IEEE 802.11k specification. It allows the administrator to set the MAC address of the client to use in the next channel load measurement request. This command must be executed from the cluster controller.

Format `wireless rrm channel-load request client [macaddr]`

Mode Privileged EXEC

Parameter	*Description*
macaddr	The client MAC address.

wireless rrm channel-load request duration

This command pertains to the Radio Resource Measurement (RRM) capabilities as described in the IEEE 802.11k specification. It allows the administrator to set the test duration to use in the next channel load measurement request. The duration value is given in terms of time units (TUs), where 1 TU equals 1024 microseconds. This command must be executed from the cluster controller.

Format `wireless rrm channel-load request duration [TUs]`

Mode Privileged EXEC

wireless rrm channel-load request send

This command pertains to the Radio Resource Measurement (RRM) capabilities as described in the IEEE 802.11k specification. It assumes that the client MAC, channel, and duration were specified by previous channel-load commands. With this information, this command sends the measurement request to the wireless client. An error will occur if the client is not associated to a managed AP within the cluster. This command must be executed from the cluster controller.

Format `wireless rrm channel-load request send`

Mode Privileged EXEC

client roam-timeout

This command configures maximum duration for which a client entry is retained in the client association database after disassociating from a managed AP. Roam-timeout is the time in seconds after disassociation for the entry to be deleted from the managed AP client association database.

Default 30 seconds

Format `client roam-timeout seconds`

Mode Wireless Config

Parameter	*Description*
roam-timeout	Time in seconds after disassociation for the entry to be deleted from the managed AP client association database.
seconds	Time in seconds from 1 to 120.

no client roam-timeout

The no version of this command returns the configured client age timeout to the default.

Format `no client roam-timeout`

Mode Wireless Config

tunnel-mtu

This command configures the network MTU size for all access points. This configuration is only used for tunneled networks and is, therefore, only available if the wireless tunneling feature is enabled. Note that the physical ports on the wireless switch and the rest of the network devices must also be configured with the appropriate MTU size. This configuration applies only to the managed access points.

Default 1500

Format `tunnel-mtu {1500 | 1520}`

Mode Wireless Config

Parameter	*Description*
1500	Maximum IP frame size is 1518 tagged/1522 untagged.
1520	Maximum IP frame size is 1538 tagged/1542 untagged.

no tunnel-mtu

The no version of this command returns the configured network MTU size to the default value.

Format `no tunnel-mtu`

Mode Wireless Config

cluster-priority

This command configures the Cluster priority of the switch. This configuration is used to change the preference level of the switch to select or unselect it as the Cluster Controller. A higher number indicates a higher preference.

Default 0

Format `cluster-priority` *`level`*

Mode Wireless Config

Parameter	*Description*
level	Preference level for Cluster Controller election.

radius server-name

This command configures global RADIUS authentication /accounting server name for wireless clients. The server name can contain alphanumeric characters plus –, _, and space.

Default
- Default-RADIUS-Server – authentication server name
- Default-RADIUS-Server – accounting server name

Format `radius server-name {auth | acct}` *`name`*

Mode Wireless Config

no radius server-name

The no version of this command sets the global RADIUS authentication /accounting server name to the default value.

Format `no radius server-name {auth | acct}`

Mode Wireless Config

Example: The following shows examples of the command.

```
(Switch) #radius server-name auth  “Wireless_Auth-Server 1” ?
<cr>    Press Enter to execute the command.

(Switch) #no radius server-name auth ?
<cr>    Press Enter to execute the command.

(Switch) #radius server-name acct  “Wireless_Acct_Server 1” ?
<cr>    Press Enter to execute the command.

(Switch) #no radius server-name acct  ?
<cr>    Press Enter to execute the command.
```

mac-authentication-mode

This command configures the client MAC authentication mode for the switch. The mode indicates whether MAC addresses in the Known Client database are granted or denied access. The MAC authentication mode is applied to the known client database configured either locally or on the RADIUS server.

Default white-list

Format `mac-authentication-mode {white-list | black-list}`

Mode Wireless Config

Parameter	*Description*
white-list	The access is granted only to clients with MACs in the Known Client database.
black-list	The access is denied to clients with MACs in the known client database.

known-client

This command configures a client MAC address in the local Known Client database. The action indicates whether to grant, deny, or use global action for MAC authentication of the client.

Format `known-client` *`macaddr`* `[name` *`name`*`] [action {global-action | grant | deny}]`

Mode Wireless Config

Parameter	*Description*
macaddr	A valid MAC address.
name	An alphanumeric string up to 32 characters in length.
global-action	Default authentication action is global-action. Apply global action to the client.
grant	Grant access to the client.
deny	Deny access to the client.

no known-client

The `no` version of this command deletes an entry from the local Known Client database.

Format `no known-client` *`macaddr`*

Mode Wireless Config

auto-ip-assign

This command pertains to the Radio Resource Measurement (RRM) capabilities as described in the IEEE 802.11k specification. It assumes that the client MAC, channel, and duration were specified by previous channel-load commands. With this information, this command sends the measurement request to the wireless client. An error will occur if the client is not associated to a managed AP within the cluster. This command must be executed from the cluster controller.

Default `Disable`

Format `auto-ip-assign`

Mode Wireless Config

no auto-ip-assign

The `no` version of this command disables auto IP address assignment mode for wireless switch.

Format `no auto-ip-assign`

Mode Wireless Config

static-ip

This command configures static IP address for the wireless switch. The IP address must be the same as an address of an active routing or loopback interface in order for the wireless function to work. If routing is disabled then the IP address must be the same as the network interface address.This IP address is used for wireless switch when auto-ip-assign mode is disabled.

Format `static-ip ipaddr`

Mode Wireless Config

Parameter	*Description*
ipaddr	A valid IP address.

no static-ip

The `no` version of this command resets the static IP address to 0.0.0.0.

Format `no static-ip`

Mode Wireless Config

show wireless

This **show** command displays the configured wireless switch global parameters and the operational status.

Format `show wireless`

Mode
- Privileged EXEC
- User EXEC

Field	*Description*
Administrative Mode	Shows whether the administrative mode is enabled.
WLAN Switch Operational Mode	Shows whether the wireless function on the switch is enabled.
WS IP Address	Shows the IP address of the switch. If the routing package is enabled, this address belongs to a routing or loopback interface.
WS Auto IP Assign Mode	Shows whether the WS Auto IP Assign mode is enabled or disabled.
WS Switch Static IP	The static IP address of the WS switch.
AP Authentication Mode	Shows whether the AP must be authenticated by using the local database or a RADIUS database.
AP Auto Upgrade Mode	Shows whether the Auto Upgrade feature is enabled or disabled.
AP Validation Method	Shows whether to use the local or RADIUS server database for AP validation.
Client Roam Timeout (secs)	Shows how long to wait before a client that disassociates from this AP or a neighbor AP must re-authenticate when it associates again.
Country Code	Shows the country in which the WLAN is operating.
Peer Group ID	Shows the Peer group ID.
Cluster Priority	Priority of this switch for the Cluster election.
Cluster Controller	Indicates whether or not this switch is the Cluster controller.
Cluster Controller IP Address	The IP address of the switch that acts as the Cluster controller.
AP Client Qos Mode	Shows whether the AP Client QoS mode is enabled or disabled.
Switch Provisioning	Shows whether Switch Provisioning is enabled or disabled.
Network Mutual Authentication Mode	Shows whether Network Mutual Authentication Mode is enabled or disabled.
Unmanaged AP Re-provisioning Mode	Shows whether Unmanaged AP Re-provisioning Mode is enabled or disabled.
Network Mutual Authentication Status	Shows the Network Mutual Authentication status.
Regenerate X.509 Certificate Status	Shows the status of regenerating the X.509 certificate.

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

```
(Switch) #show wireless

Administrative Mode.......................... Enable
WLAN Switch Operational Mode................. Enabled
WS IP Address................................ 10.0.0.1
WS Auto IP Assign Mode....................... Disable
WS Switch Static IP.......................... 2.2.2.2
AP Authentication Mode....................... Disable
AP Auto Upgrade Mode......................... Disable
AP Validation Method......................... Local
Client Roam Timeout (secs)................... 30
Country Code................................. US - United States
Peer Group ID................................ 1
WIDS Priority................................ 2
Cluster Controller........................... Yes
Cluster Controller IP Address................ 10.0.0.1
AP Client QoS Mode........................... Disable
Switch Provisioning.......................... Disable
Network Mutual Authentication Mode........... Disable
Unmanaged AP Re-provisioning Mode............ Disable
Network Mutual Authentication Status......... Not Started
Regenerate X.509 Certificate Status.......... Not In Progress
```

show wireless country-code

This **show** command displays the country codes configurable on the Wireless Switch.

Format `show wireless country-code`

Mode Privileged EXEC

Field	*Description*
Code	Shows the 2-letter country code.
Country	Shows the name of the country associated with the code.

show wireless OUI database

This **show** command displays all the OUI entries created by the admin in the local OUI database.

Format `show OUI database [ouival]`

Mode Privileged EXEC

Field	*Description*
ouival	OUI Value of the vendor of AP/Client.
oui	Organization name for the OUI.

Example:

```
OUI Value             OUI Description
--------------------  -------------------------------
00:11:11
00:11:12              Andreys OUI
```

show wireless discovery

This **show** command displays the configured Wireless Switch discovery methods.

Format `show wireless discovery`

Mode Privileged EXEC

Field	*Description*
IP Polling Mode	Shows whether the L3 IP Polling discovery method is enabled.
L2 Multicast Discovery Mode	Shows whether the L2 Multicast Discovery Mode is enabled.

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

```
(Switch) #show wireless discovery

IP Polling Mode.............................. Enabled
L2 Multicast Discovery Mode.................. Enabled
```

show wireless discovery ip-list

This **show** command displays the configured Wireless Switch IP polling list and the polling status for each configured IP address for discovery.

Format `show wireless discovery ip-list`

Mode Privileged EXEC

Field	*Description*
IP Address	Shows the IP addresses configured in the L3/IP Discovery List.
Status	Shows the L3 discovery status. Possible values are *Not Polled*, *Unreachable*, or *Discovered*.

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

```
(Switch) #show wireless discovery ip-list

IP Address       Status
---------------- ------------
1.1.1.1          Not Polled
```

show wireless discovery vlan-list

This **show** command displays the configured VLAN ID list for L2 discovery.

Format `show wireless discovery vlan-list`

Mode Privileged EXEC

Field	*Description*
VLAN	Shows the ID and name of each VLAN in the L2 Discovery list.

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

```
(Switch) #show wireless discovery vlan-list

VLAN
----------------
– Default
```

show wireless l2tunnel vlan-list

This **show** command displays the configured tunneled VLANs for centralized L2 tunneling.

Format `show wireless l2tunnel vlan-list`

Mode Privileged EXEC

Field	*Description*
VLAN	Shows the ID and name of each VLAN in the L2 tunneling list.

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

```
(Switch) #show wireless l2tunnel vlan-list

VLAN
----------------
1 – Default
```

show wireless status

This **show** command displays the configured global Wireless Switch status parameters. The counters are aggregated for all switches in the cluster when the switch acts as the Cluster Controller. Otherwise the values are for this switch only. The limits are for the whole cluster.

Format `show wireless status`

Mode Privileged EXEC

Field	*Description*
Total Access Points	The total number of access points in the managed AP database. This value is always equal to the sum of Managed Access Points, Connection Failed Access Points, and Discovered Access Points.
Managed Access Points	The total number of APs in the managed AP database that are authenticated, configured, and have an active connection with the Wireless Switch.
Connection Failed Access Points	The number of APs that were previously authenticated and managed, but lost connection with the Wireless Switch.
Discovered Access Points	APs that have a connection with the switch, but have not yet been completely configured (i.e., managed APs with a discovered or authenticated status).
Maximum Managed APs in Peer Group	The maximum number of APs that can be managed in the peer group.
Rogue AP Mitigation Count	Number of APs to which the wireless system is currently sending de-authentication messages to mitigate against rogue APs.
Rogue AP Mitigation Limit	Maximum number of APs for which the system can send de-authentication frames.
Total Clients	The sum total of the number of clients that are either authenticated or disassociated.
Associated Clients	Total number of clients in the database. This total includes clients with an Associated, Authenticated or Disassociated status.
Authenticated Clients	Total number of clients in the associated client database with an *Authenticated* status.
Maximum Associated Clients	Maximum number of clients that can be authenticated in the peer group.
Detected Clients	The number of clients that are detected by the wireless switch through RF scan mechanism.
Maximum Detected Clients	The maximum number of clients that can be stored on the wireless switch.
Peer Switches	Total number of peer WLAN switches detected on the network.
Unknown Access Points	Total number of APs that are detected and classified as Unknown on the WLAN switch. These includes rogue APs and APs not connected to the network.
Rogue Access Points	Total number of rogue APs currently detected on the WLAN.
Standalone Access Points	Total number of trusted APs in standalone mode.
AP Provisioning Count	Total number of entries in the AP provisioning database.

Field	*Description*
Maximum AP Provisioning Entries	Total number of APs that can be provisioned.
Distributed Tunnel Clients	Total number of clients that are currently sending and receiving packets via distributed tunnels.
WLAN Utilization	Total network utilization across all APs managed by this switch, this is an average of the global statistics received from each AP.
Maximum Pre-authentication History Entries	Maximum number of client pre-authentication events that can be recorded by the system.
Total Pre-authentication History Entries	Total number of client pre-authentication events that are currently recorded by the system.
Maximum Roam History Entries	Maximum number of roam history entries that can be recorded for all detected clients.
Total Roam History Entries	Total number of roam history events that are currently recorded by the system.

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

```
(Switch) #show wireless status

Total Access Points..........................  3
Managed Access Points........................  3
Connection Failed Access Points..............  0
Discovered Access Points.....................  0
Maximum Managed APs in Peer Group............  96
Rogue AP Mitigation Count....................  0
Rogue AP Mitigation Limit....................  16
Total Clients................................  1
Authenticated Clients........................  1
Maximum Associated Clients...................  4000
Detected Clients.............................  44
Maximum Detected Clients.....................  8000
Peer Switches................................  1
Unknown Access Points........................  9
Rogue Access Points..........................  3
Standalone Access Points.....................  0
AP Provisioning Count........................  5
Maximum AP Provisioning Entries..............  192
Distributed Tunnel Clients...................  0
WLAN Utilization.............................  10%
Maximum Pre-authentication History Entries.....  500
Total Pre-authentication History Entries.......  0
Maximum Roam History Entries.................  500
Total Roam History Entries...................  27
```

show wireless statistics

This **show** command displays the current global Wireless Switch statistics.

Format `show wireless statistics`

Mode Privileged EXEC

Field	*Description*
WLAN Bytes Received	Shows the total bytes received across all APs managed by the switch.
WLAN Bytes Transmitted	Shows the total bytes transmitted across all APs managed by the switch.
WLAN Packets Received	Shows the total number of packets received across all APs managed by the switch.
WLAN Packets Transmitted	Shows the total number of packets transmitted across all APs managed by the switch.
WLAN Bytes Received Dropped	Shows the total bytes received across all APs managed by the switch and dropped.
WLAN Bytes Transmit Dropped	Shows the total bytes transmitted across all APs managed by the switch and dropped.
WLAN Packets Receive Dropped	Shows the total number of packets received across all APs managed by the switch and dropped.
WLAN Packets Transmit Dropped	Shows the total number of packets transmitted across all APs managed by the switch and dropped.

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

```
(Switch) #show wireless statistics <cr>
WLAN Bytes Received..............................0
WLAN Bytes Transmitted...........................0
WLAN Packets Received............................0
WLAN Packets Transmitted.........................0
WLAN Bytes Receive Dropped.......................0
WLAN Bytes Transmit Dropped......................0
WLAN Packets Receive Dropped.....................0
WLAN Packets Transmit Dropped....................0
```

show wireless switch status

This **show** command displays the current global Wireless Switch status parameters. If the Wireless Switch is a Cluster Controller, then this command shows per-switch status parameters for all the switches in the wireless network. For the switch that is not acting as a Cluster Controller, only the local status parameters are displayed.

Format `show wireless switch {ipaddr | local} status`

Mode Privileged EXEC

The following table lists the command parameters

Parameter	*Description*
ipaddr	IP address of the Wireless Switch in the wireless system.

The following table lists the output fields that display.

Field	*Description*
Switch IP Address	IP address of the Wireless Switch or any peer switch in the wireless system.
Cluster Priority	Priority of this switch for the Cluster election.
Total Access Points	The total number of access points in the managed AP database. This value is always equal to the sum of Managed Access Points, Connection Failed Access Points, and Discovered Access Points.
Managed Access Points	The total number of APs in the managed AP database that are authenticated, configured, and have an active connection with the Wireless Switch.
Connection Failed Access Points	The number of APs that were previously authenticated and managed, but lost connection with the Wireless Switch.
Discovered Access Points	APs that have a connection with the Wireless Switch, but have not yet been completely configured (i.e. managed APs with a discovered or authenticated status).
Maximum Managed Access Points	The maximum number of managed access points supported by the switch.
Total Clients	Total number of clients in the database. This total includes clients with an Associated, Authenticated, or Disassociated status.
Authenticated Clients	Total number of clients in the associated client database with an Authenticated status.
Distributed Tunnel Clients	Number of clients that are currently sending and receiving packets via distributed tunnels.
WLAN Utilization	Total network utilization across all APs managed by this switch, this is an average of the global statistics received from each AP.

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

If a network consists of two switches 192.168.37.60 and 192.168.37.61 respectively and the former is the Cluster Controller, this command works differently at Cluster Controller and peer switch that is not acting as a Cluster Controller as follows.

On the Cluster Controller, it displays entries in the following format:

```
(Switch) show wireless switch 10.27.65.8 status

Switch IP Address.............................. 10.27.65.8
Cluster Priority............................... 1
Total Access Points............................ 0
Managed Access Points.......................... 0
Connection Failed Access Points................ 0
Discovered Access Points....................... 0
Maximum Managed Access Points.................. 64
Total Clients.................................. 0
Authenticated Clients.......................... 0
Distributed Tunnel Clients..................... 0
WLAN Utilization............................... 0%
```

On the switch that is not acting as a Cluster Controller the summary command displays entries in the following format:

```
(Switch) #show wireless switch 192.168.37.60 status
Error! Only Cluster Controller can display the peer switch status parameters.

(Switch) #show wireless switch 192.168.37.61 status
Switch IP Address.............................. 192.168.37.61
Cluster Priority............................... 1
Total Access Points............................ 5
Managed Access Points.......................... 3
Connection Failed Access Points................ 1
Discovered Access Points....................... 1
Total Clients.................................. 3
Associated Clients............................. 1
Authenticated Clients.......................... 2
Standalone Access Points....................... 0
WLAN Utilization............................... 10 %
```

show wireless switch statistics

This **show** command displays the current Wireless Switch statistics. If the Wireless Switch is a Cluster Controller, then this command shows per switch statistics for all the switches in the wireless system. For the switch that is not acting as a Cluster Controller, only the local statistics are displayed.

Format `show wireless switch {ipaddr | local} statistics`

Mode Privileged EXEC

Field	*Description*
ipaddr	IP address of the Wireless Switch in the wireless system.

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

If a network consists of two switches 192.168.37.60 and 192.168.37.61 respectively and former is the Cluster Controller, this command works differently at Cluster Controller and the peer switch which is not a Cluster Controller as follows.

On the Cluster Controller, it displays entries in the following format:

```
(Switch) #show wireless switch 192.168.37.60 statistics <cr>

WLAN Bytes Received..................................... 1873
WLAN Bytes Transmitted.................................. 8234
WLAN Packets Received................................... 233
WLAN Packets Transmitted................................ 435
WLAN Bytes Receive Dropped.............................. 0
WLAN Bytes Transmit Dropped............................. 0
WLAN Packets Receive Dropped............................ 0
WLAN Packets Transmit Dropped........................... 0

(Switch) #show wireless switch 192.168.37.61 statistics <cr>

WLAN Bytes Received..................................... 320
WLAN Bytes Transmitted.................................. 560
WLAN Packets Received................................... 45
WLAN Packets Transmitted................................ 78
WLAN Bytes Receive Dropped.............................. 0
WLAN Bytes Transmit Dropped............................. 0
WLAN Packets Receive Dropped............................ 0
WLAN Packets Transmit Dropped........................... 0
```

On the switch that is not acting as a Cluster Controller the summary command displays entries in the following format:

```
(Switch) #show wireless switch 192.168.37.60 statistics <cr>
Error! Only Cluster Controller can display the peer switch statistics.
(Switch) #show wireless switch 192.168.37.61 statistics <cr>

WLAN Bytes Received..................................... 320
WLAN Bytes Transmitted.................................. 560
WLAN Packets Received................................... 45
WLAN Packets Transmitted................................ 78
WLAN Bytes Receive Dropped.............................. 0
WLAN Bytes Transmit Dropped............................. 0
WLAN Packets Receive Dropped............................ 0
WLAN Packets Transmit Dropped........................... 0
```

The local switch statistics can also be displayed using the following command format:

```
(Switch) #show wireless switch local statistics <cr>

WLAN Bytes Received..................................... 320
WLAN Bytes Transmitted.................................. 560
WLAN Packets Received................................... 45
WLAN Packets Transmitted................................ 78
WLAN Bytes Receive Dropped.............................. 0
WLAN Bytes Transmit Dropped............................. 0
WLAN Packets Receive Dropped............................ 0
WLAN Packets Transmit Dropped........................... 0
```

show wireless switch tspec status

This **show** command displays the wireless switch TSPEC status parameters. If the wireless switch is a Cluster controller, then this command shows per switch status parameters for all the switches in the wireless network. For the switch that is not acting as a Cluster controller, only the local status parameters are displayed.

Format `show wireless switch {ipaddr | local} tspec status`

Mode Privileged EXEC

Field	*Description*
ipaddr	IP address of the switch in the wireless system.
IP Address	IP address of the wireless system. For the Cluster controller, this can be any peer switch in the wireless system.
Total Voice Traffic Streams	Total number of traffic streams in effect for the voice access category on the wireless switch.
Total Video Traffic Streams	Total number of traffic streams in effect for the video access category on the wireless switch.
Total Traffic Stream Clients	Total number of individual clients that have one or more traffic streams in effect on the wireless switch. This value is inclusive of the Total Traffic Stream Roaming Clients listed below.
Total Traffic Stream Roaming Clients	Total number of individual clients, that were associated via roaming, that have one or more traffic streams in effect on the wireless switch.

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

```
(Switch) #show wireless switch 192.168.37.61 tspec status

Switch IP Address.............................. 192.168.37.61
Total Voice Traffic Streams.................... 0
Total Video Traffic Streams.................... 0
Total Traffic Stream Clients................... 0
Total Traffic Stream Roaming Clients........... 0
```

show wireless switch tspec statistics

This **show** command displays the wireless switch TSPEC statistics. If the wireless switch is a Cluster controller, then this command shows per switch status parameters for all the switches in the wireless network. For the switch that is not acting as a Cluster controller, only the local status parameters are displayed.

Format `show wireless switch {ipaddr | local} tspec statistics`

Mode Privileged EXEC

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

```
(Switch) #show wireless switch 192.168.37.61 tspec statistics

Switch IP Address.............................. 192.168.37.61

Access Category................................ Voice
Total TSPEC Packets Received................... 0
Total TSPEC Packets Transmitted................ 0
Total TSPEC Bytes Received..................... 0
Total TSPEC Bytes Transmitted.................. 0
```

```
Total TSPECs Accepted..................... 0
Total TSPECs Rejected..................... 0
Total Roaming TSPECs Accepted............. 0
Total Roaming TSPECs Rejected............. 0

Access Category........................... Video
Total TSPEC Packets Received.............. 0
Total TSPEC Packets Transmitted........... 0
Total TSPEC Bytes Received................ 0
Total TSPEC Bytes Transmitted............. 0
Total TSPECs Accepted..................... 0
Total TSPECs Rejected..................... 0
Total Roaming TSPECs Accepted............. 0
Total Roaming TSPECs Rejected............. 0
```

show wireless trapflags

This **show** command displays the configured Wireless Switch SNMP trap modes.

Format `show wireless trapflags`

Mode Privileged EXEC

Field	*Description*
AP Failure Traps	Shows whether AP Failure Traps are enabled.
AP State Change Traps	Shows whether AP State Change Traps are enabled.
Client Failure Traps	Shows whether Client Failure Traps are enabled.
Client State Change Traps	Shows whether Client State Change Traps are enabled.
Peer Switch Traps	Shows whether Peer Switch Traps are enabled.
RF Scan Traps	Shows whether RF Scan Traps are enabled.
Rogue AP Traps	Shows whether Rogue AP Traps are enabled.
WIDS Status Traps	Shows whether WIDS Status Traps are enabled.
Wireless Status Traps	Shows whether Wireless Status Traps are enabled.

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

```
(Switch) #show wireless trapflags
AP Failure Traps.............................. Disable
AP State Change Traps......................... Disable
Client Failure Traps.......................... Disable
Client State Change Traps..................... Disable
Peer Switch Traps............................. Disable
RF Scan Traps................................. Disable
Rogue AP Traps................................ Disable
TSPEC Traps................................... Disable
WIDS Status Traps............................. Disable
Wireless Status Traps......................... Disable
```

show trapflags (Global Wireless Status)

The existing DWS-4000 **show trapflags** command is modified to show the global Wireless Switch trap configuration. See the command "show trapflags" on page 92.

show wireless tspec global

This show command displays the configured wireless switch TSPEC global parameters.

Format	`show wireless tspec global`
Mode	Privileged EXEC

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

```
(Switch) #show wireless tspec global

Violation Report Interval..................... 300
```

show wireless tspec status

This show command displays the configured wireless switch TSPEC global status. If the wireless switch is a Cluster Controller, then the values displayed by this command represent the aggregate for the entire cluster of peer switches.

Format	`show wireless tspec status`
Mode	Privileged EXEC

Field	*Description*
Total Voice Traffic Streams	Total number of traffic streams in effect for the voice access category on the wireless switch.
Total Video Traffic Streams	Total number of traffic streams in effect for the video access category on the wireless switch.
Total Traffic Stream Clients	Total number of individual clients that have one or more traffic streams in effect on the wireless switch. This value is inclusive of the **Total Traffic Stream Roaming Clients** listed below.
Total Traffic Stream Roaming Clients	Total number of individual clients, that were associated via roaming, that have one or more traffic streams in effect on the wireless switch.

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

```
(Switch) #show wireless tspec status

Total Voice Traffic Streams.................... 0
Total Video Traffic Streams.................... 0
Total Traffic Stream Clients................... 0
Total Traffic Stream Roaming Clients........... 0
```

show wireless tspec statistics

This show command displays the configured wireless switch TSPEC global statistics. If the wireless switch is a Cluster Controller, then the values displayed by this command represent the aggregate for the entire cluster of peer switches.

Format `show wireless tspec statistics`

Mode Privileged EXEC

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

```
(Switch) #show wireless tspec statistics

Access Category.............................. Voice
Total TSPEC Packets Received................. 0
Total TSPEC Packets Transmitted.............. 0
Total TSPEC Bytes Received................... 0
Total TSPEC Bytes Transmitted................ 0
Total TSPECs Accepted........................ 0
Total TSPECs Rejected........................ 0
Total Roaming TSPECs Accepted................ 0
Total Roaming TSPECs Rejected................ 0

Access Category.............................. Video
Total TSPEC Packets Received................. 0
Total TSPEC Packets Transmitted.............. 0
Total TSPEC Bytes Received................... 0
Total TSPEC Bytes Transmitted................ 0
Total TSPECs Accepted........................ 0
Total TSPECs Rejected........................ 0
Total Roaming TSPECs Accepted................ 0
Total Roaming TSPECs Rejected................ 0
```

show wireless tunnel-mtu

This **show** command displays the configured network MTU size. This is a global configuration for all managed access points.

Format `show wireless tunnel-mtu`

Mode Privileged EXEC

show wireless agetime

This **show** command displays the configured age times for the status database entries.

Format `show wireless agetime`

Mode Privileged EXEC

Field	*Description*
Ad Hoc Client Status Age (hours)	Shows how long to continue to display an ad hoc client in the status list since it was last detected.
AP Failure Status Age (hours)	Shows how long to continue to display a failed AP in the status list since it was last detected.
RF Scan Status Age (hours)	Shows how long to continue to display an AP detected through the RF Scan since it was last detected.
Detected Clients Age (hours)	Shows how long to keep an entry in the Detected Client Status list.
AP Provisioning Database Age Time (hours)	This value determines how long to keep an entry in the AP Provisioning Database. After an AP is inactive for the number of hours you specify in this field, its entry is removed from the database. Range is 0 to 40. If set to 0, entries are not aged-out and remain in the database forever.

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

```
(Switch) #show wireless agetime <cr>
Ad Hoc Client Statue Age (hours)..............  24
AP Failure Status Age (hours).................  24
RF Scan Status Age (hours)....................  24
Detected Clients Age (hours)..................24
AP Provisioning Database Age Time (hours).....24
```

show wireless peer-switch configuration

This show command displays the peer switch configuration groups mode.

Format `show wireless peer-switch configuration`

Mode Privileged EXEC

Field	*Description*
AP Database	Displays whether the AP database configuration push to peer switches is enabled or disabled.
AP Profile	Displays whether the AP profile and network configuration push to peer switches is enabled or disabled.
Channel Power	Displays whether the channel and power configuration push to peer switches is enabled or disabled.
Discovery	Displays whether the discovery configuration push to peer switches is enabled or disabled.
Global	Displays whether the global configuration push to peer switches is enabled or disabled.
Known Client	Displays whether the known client database push to peer switches is enabled or disabled.
Captive Portal	Displays whether Captive Portal configuration push to peer switches is enabled or disabled.
Radius Client	Displays whether RADIUS client configuration push to peer switches is enabled or disabled.
QoS ACL	Displays whether QoS ACL configuration push to peer switches is enabled or disabled.

Field	*Description*
QoS DiffServ	Displays whether QoS DiffServ (classes, services, and policies) configuration push to peer switches is enabled or disabled.

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

```
(Switch) #show wireless peer-switch configuration

AP Database..................................... Enable
AP Profile...................................... Enable
Channel Power................................... Enable
Discovery....................................... Disable
Global.......................................... Enable
Known Client.................................... Enable
Captive Portal.................................. Enable
RADIUS Client................................... Enable
QoS ACL......................................... Enable
QoS DiffServ.................................... Enable
```

show wireless configuration request status

This show command displays the global peer switch configuration push status and configuration push status for all peer switches.

Format `show wireless configuration request status`

Mode Privileged EXEC

Field	*Description*
Status	The global status for the configuration push request.
Total Count	The total number of peer switches configuration being pushed in the current configuration push request. This may be to one peer switch or to the total number of peer switches at the time the configuration push request is started.
Success Count	Indicates the total number of peer switches to which the configuration has been pushed successfully for the current configuration push request.
Failure Count	Indicates the total number of peer switches to which the configuration push request failed for the current configuration push request.
IP Address	The peer switch IP Address.
Configuration Status	Configuration push status for the peer switch.

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

```
(Switch) #show wireless configuration request status
Global Status:
Configuration Status.................. Sending Configuration
Total Count         ................... 3
Success Count  ....................... 0
Failure Count ........................ 1
```

```
Peer-Switch Status:
IP Address         Configuration Status
---------------    --------------------
10.0.0.100         Failure Invalid Code Version
10.0.0.101         In Progress
10.0.0.102         Requested
```

show wireless configuration receive status

This show command displays the peer switch configuration received status.

Format `show wireless configuration receive status`

Mode Privileged EXEC

Field	*Description*
Switch IP	The peer switch IP address that pushed configuration.
Configuration Received	Indicates the configuration groups received as part of the configuration push.
Receive Time	Indicates the configuration push received time.
Receive Status	Indicates the status of the configuration push receive from the peer switch.

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

```
(Switch) #show wireless configuration receive status

Switch IP.........................  192.168.30.20
Configuration Received .............AP Database,
                                    AP Profile,
                                    Channel Power,
                                    Discovery,
                                    Global,
                                            Known-Client
Receive Time .......................JAN 03 23:32:06 1970
Receive Status .....................Failure Invalid Configuration
```

show wireless ap capability

This command displays access point hardware type and radio hardware type capabilities. If no parameters are specified, a summary of access point hardware type capabilities for all supported AP hardware types is displayed. If an AP hardware type ID and radio interface is specified, the detailed hardware type capabilities are displayed.

Format `show wireless ap capability [hw-id radio radio-id]`

Mode Privileged EXEC

Field	*Description*
hw-id	The AP hardware type ID. The range is 1–6
radio-id	The radio index on the AP hardware type.
Hardware Type ID	AP hardware type that supports this radio.
Hardware Type Description	Descriptive name of the AP hardware type.
Radio Count	Number of radios supported on the AP.
Image Type	AP image type ID and description.
Radio	The radio index of this radio in the AP.
Radio Type Description	Text description of this radio type.
VAP Count	Number of virtual access points supported by this radio.
802.11a Support	Flag indicating whether this radio supports 802.11a Mode.
802.11bg Support	Flag indicating whether this radio supports 802.11bg Mode.
802.11n Support	Flag indicating whether this radio supports 802.11n configuration parameters.

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

```
(Switch) #show wireless ap capability

Hardware Type ID    Hardware Type Description          Radio Count   Image Type
-----------------  ---------------------------------- ------------  ----------
    3              MJ Dual Radio Broadcom a/b/g         2             2
    4              MJ Single Radio Broadcom a/b/g       1             2
    5              MJ Dual Radio Broadcom a/b/g/n       2             2
    6              MJ Single Radio Broadcom a/b/g/n     1             2

(Switch) #

(Switch) #show wireless ap capability 6 radio 1

Hardware Type ID ..................... 6
Hardware Type Description............ MJ Single Radio Broadcom a/b/g/n
Radio Count.........................1
Image Type.......................... 1-MJ Development Board

Radio...............................1
Radio Type Description..............Broadcom a/b/g/n
```

```
VAP Count.............................8
802.11a Support.......................Enable
802.11bg Support......................Enable
802.11n Support......................Enable
```

show wireless ap image-capability

This command displays the access point image capability table.

Format `show wireless ap image-capability`

Mode Privileged EXEC

Field	*Description*
Image Type ID	AP image type ID.
Image Type Description	Descriptive name of the AP image type.

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

```
(Switch) #show wireless ap image-capability

Image Type ID   Image Type Description
--------------  ----------------------
1               MJ Development Board Atheros Radios
2               MJ Development Board Broadcom Radios
```

show wireless ap image availability

This command displays the code version information of the wireless switch stored access point images.

Format `show wireless ap image availability`

Mode Privileged EXEC

Field	*Description*
AP Image Type ID	AP Image ID
Code Version	Version of AP image corresponding to the image ID.

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

```
(Switch) #show wireless ap image availability

AP Image Type   Code Version
-------------   ------------
    1           10.2.0.2
    2           10.2.0.1
```

show wireless mac-authentication-mode

This show command displays the configured client MAC authentication mode for the switch.

Format `show wireless mac-authentication-mode`

Mode Privileged EXEC

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

```
(Switch) # show wireless mac-authentication-mode
MAC Authentication Action..................... white-list
```

show wireless known-client

This show command displays the content of the local Known Client database or an entry of the local Know Client database.

Format `show wireless known-client [macaddr]`

Mode Privileged EXEC

Field	*Description*
`macaddr`	The client MAC address in the local Known Client database.
Nickname	An alphanumeric string up to 32 characters in length.
Action	Indicates whether to grant, deny, or use global action for MAC authentication of the client.

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

```
(Switch) #show wireless known-client

MAC Address           Nickname      Action
-------------------------------------------------
10:10:10:10:10:10     client1       grant
```

show wireless radius

This show command displays the configured global RADIUS configuration for wireless clients.

Format `show wireless radius`

Mode Privileged EXEC

Field	*Description*
RADIUS Authentication Server Name	The name of the RADIUS server used for AP authentications as well as client authentications when a network-level RADIUS server is not defined.
RADIUS Authentication Server Configured	Indicates whether the specified named RADIUS Authentication server is configured in the RADIUS Client configuration.
RADIUS Accounting Server Name	The name of the RADIUS server used for reporting wireless client associations and disassociations when a network-level RADIUS accounting server is not defined.
RADIUS Accounting Server Configured	Indicates whether the specified named RADIUS Accounting server is configured in the RADIUS Client configuration.
RADIUS Accounting	Flag to indicate whether or not RADIUS accounting is enabled for wireless clients accounting.

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

```
(Switch) #show wireless radius
RADIUS Authentication Server Name.......... Default-RADIUS-Server
RADIUS Authentication Server Configured.... Configured
RADIUS Accounting Server Name ............. Default-RADIUS-Server
RADIUS Accounting Server Configured........ Not Configured
RADIUS Accounting ......................... Disable
```

show wireless rrm channel-load current-request

This show command displays the current request for channel load measurements from clients for Radio Resource Measurement (RRM).

Format `show wireless rrm channel-load current-request`

Mode Privileged EXEC

Field	*Description*
AP	The MAC address of the managed AP associated with client.
Client	The MAC address of the client performing the load measurement.
Channel	The channel used by the client.
Duration	The duration of the request as performed by the client, expressed in TUs (time units), as defined by the 802.11k specification. Each TU equals 1024 microseconds.

Field	*Description*
Time Remaining	The time remaining for the switch to receive the channel load measurement message from the client.
Status	The result of the measurement, if the request is not in progress. Possible values are: • **None**. No request is pending, or has been submitted. • **In Progress**. The current request is in progress. • **Aborted**. The current request was terminated before its completion. • **Timed Out**. The response from the current request was not received 60 seconds after the request was submitted. • **Incapable**. The client was incapable of fulfilling the request. • **Refused**. The client refused to fulfill the request.

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

```
(Switch) #show wireless rrm channel-load current-request
AP : 0C:22:38:57:63:D0   Client : 52:27:3A:BB:C7:E0
Channel: 23 Duration (in TUs):  444 Time Remaining:0d:00:00:00
Status: Aborted
```

show wireless rrm channel-load history

This show command displays summary information about all known Radio Resource Measurement (RRM) channel load measurement reports.

Format `show wireless rrm channel-load history`

Mode Privileged EXEC

Field	*Description*
Age	Ages of earliest and latest reports, in seconds.
Channel Load	The measured level of utilization of the channel.
Channel	The channel used by the client.
Mode	The mode, or result, as defined by the IEEE 802.11k specification. This field can be one of the following values: • **Success**. The load measurement was successful. • **Incapable**. The client could not fulfill the request. • **Refused**. The client refused the request. • **Late**. The response from the client failed to be retrieved in the allotted duration of measurement time.
Duration	The duration of the request as performed by the client, expressed in TUs (time units), as defined by the 802.11k specification. Each TU equals 1024 microseconds.

Field	*Description*
Status	The result of the measurement, if the request is not in progress. Possible values are: • **None**. No request is pending, or has been submitted. • **In Progress**. The current request is in progress. • **Aborted**. The current request was terminated before its completion. • **Timed Out**. The response from the current request was not received 60 seconds after the request was submitted. • **Incapable**. The client was incapable of fulfilling the request. • **Refused**. The client refused to fulfill the request.

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

```
(Switch) #show wireless rrm channel-load history

Number of reports = 4  Age of earliest = 0d:00:00:17  Age of latest = 0d:00:00:08
Channel load: min/avg/max =   16/16/16 %
Successful measurements   =   3
Faulty measurements       =   1
  Too late from client:       0
  Incapable clients:          0
  Refused by client:          1
```

show wireless rrm channel-load history detail

This show command displays detailed information about each known Radio Resource Measurement (RRM) channel load measurement report.

Format `show wireless rrm channel-load history detail`

Mode Privileged EXEC

Field	*Description*
Age	Ages of earliest and latest reports, in seconds.
Channel Load	The measured level of utilization of the channel.
Channel	The channel used by the client.
Mode	The *mode*, or result, as defined by the IEEE 802.11k specification. This field can be one of the following values: • **Success**. The load measurement was successful. • **Incapable**. The client could not fulfill the request. • **Refused**. The client refused the request. • **Late**. The response from the client failed to be retrieved in the allotted duration of measurement time.
Duration	The duration of the request as performed by the client, expressed in TUs (time units), as defined by the 802.11k specification. Each TU equals 1024 microseconds.

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

```
(Switch) #show wireless rrm channel-load history detail

Number of reports = 4  Age of earliest = 0d:00:00:28  Age of latest = 0d:00:00:19
Channel load: min/avg/max =   16/16/16 %
Successful measurements   =   3
Faulty measurements       =   1
  Too late from client:       0
  Incapable clients:          0
  Refused by client:          1

--------------------------------
Report #1   Age: 0d:00:00:19
AP: 01:02:03:04:05:06   Client: 06:05:04:03:02:01
Duration:          444 Channel: 23
Load:              16%    Mode: REFUSED
--------------------------------
Report #2   Age: 0d:00:00:22
AP: 01:02:03:04:05:06   Client: 06:05:04:03:02:01
Duration:          444 Channel: 23
Load:              16%    Mode: Success
--------------------------------
Report #3   Age: 0d:00:00:25
AP: 01:02:03:04:05:06   Client: 06:05:04:03:02:01
Duration:          444 Channel: 23
Load:              16%    Mode: Success
--------------------------------
Report #4   Age: 0d:00:00:28
AP: 01:02:03:04:05:06   Client: 06:05:04:03:02:01
Duration:          444 Channel: 23
Load:              16%    Mode: Success
--------------------------------
```

show wireless rrm neighbors ap

This show command displays the current neighbor lists for Radio Resource Measurement (RRM). This command can be invoked to show either all neighbor information, or information related to one managed AP.

Format `show wireless rrm neighbors [ap macaddr]`

Mode Privileged EXEC

Field	*Description*
`macaddr`	The MAC address of the neighbor AP with the information to display.

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

```
(Switch) #show wireless rrm neighbors

AP                 Radio VAP  Neighbors
00:1B:E9:16:37:40      1   0  1- 00:1B:E9:16:27:40
                              2- 00:1B:E9:16:27:90
00:1B:E9:16:37:40      1   3  1- 00:1B:E9:16:27:40
                              2- 00:1B:E9:16:27:90
```

```
00:1B:E9:16:37:40      1   9  1- 00:1B:E9:16:27:40

(Switch) #show wireless rrm neighbors ap 00:1b:e9:16:37:40

 AP:  00:1B:E9:16:37:40 Radio/VAP: 1/0 (00:1B:E9:16:37:40)
============================================================

    Neighbor      Chnl RSSI      Age      SSID
----------------- ---- ---- ------------ -----------------
00:1B:E9:16:27:40   11  100   0d:00:00:17 Marketing Dept
00:1B:E9:16:27:90   11  100   0d:00:00:17 Marketing Dept

 AP:  00:1B:E9:16:37:40 Radio/VAP: 1/3 (00:1B:E9:16:37:43)
============================================================

    Neighbor      Chnl RSSI      Age      SSID
----------------- ---- ---- ------------ -----------------
00:1B:E9:16:27:40   11  100   0d:00:00:17 Marketing Dept
00:1B:E9:16:27:90   11  100   0d:00:00:17 Marketing Dept

 AP:  00:1B:E9:16:37:40 Radio/VAP: 1/9 (00:1B:E9:16:37:49)
============================================================

    Neighbor      Chnl RSSI      Age      SSID
----------------- ---- ---- ------------ -----------------
00:1B:E9:16:27:40   11  100   0d:00:00:17 Marketing Dept
```

show wireless mac-authentication-mode

This show command displays the configured client MAC authentication mode for the switch.

Format	`show wireless mac-authentication-mode`
Mode	Privileged EXEC

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

```
(Switch) # show wireless mac-authentication-mode
MAC Authentication Action..................... white-list
```

show wireless known-client

This show command displays the content of the local Known Client database or an entry of the local Known Client database.

Format `show wireless known-client [macaddr]`

Mode Privileged EXEC

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

```
(Switch) #show wireless known-client
MAC Address           Nickname       Action
---------------------------------------
10:10:10:10:10:10   client1          grant
```

clear wireless statistics

This **clear** command resets the global Wireless Switch statistics.

Format `clear wireless statistics`

Mode Privileged EXEC

Example: The following shows an example of the command.

```
(Switch) #clear wireless statistics
Are you sure you want to clear the wireless switch statistics? (y/n) y
Sent clear statistics request to the wireless switch.
The statistics are not cleared immediately.

(Switch) #clear wireless statistics
Are you sure you want to clear the wireless switch statistics? (y/n) n
Wireless switch statistics not cleared.
```

wireless acknowledge-rogue

Use this command to clear the rogue AP state in the RF Scan database for the specified AP. If you do not specify a MAC address, the rogue AP state will be cleared for all rogue APs.

Format `wireless acknowledge-rogue [macaddr]`

Mode Privileged Exec

dist-tunnel idle-timeout

Use this command to globally configure the time interval for which L2 distributed tunneled clients can stay idle. Beyond this time interval, the tunnel is terminated. The parameter idle-timeout is a numeric value in seconds.

Default 120

Format `dist-tunnel idle-timeout seconds`

Mode Wireless Config

Parameter	*Description*
`seconds`	The identifier for idle-timeout. The range is 30 to 3600 seconds.

dist-tunnel max-timeout

Use this command to globally configure the maximum time for the L2 distributed tunneled clients beyond which the tunnel is terminated. The parameter max-timeout is a numeric value in seconds.

Default 7200

Format `dist-tunnel max-timeout seconds`

Mode Wireless Config

Parameter	*Description*
`seconds`	The identifier for max-timeout. The range is 30 to 86400 seconds.

dist-tunnel mcast-repl

Use this command to globally configure the maximum multicast replications allowed for the L2 distributed tunneled clients. The parameter *`mcast-repl`* is a numeric value.

Default 128

Format `dist-tunnel mcast-repl` *`mcast-repl`*

Mode Wireless Config

Parameter	*Description*
mcast-repl	The identifier for multicast replications. The range is 1 to 1024.

dist-tunnel max-clients

Use this command to globally configure the maximum number of clients that can be tunneled using L2 distributed tunnels. The parameter `max-value` is a numeric value.

Default 128

Format `dist-tunnel max-clients max-value`

Mode Wireless Config

Parameter	*Description*
`max-value`	The identifier for maximum clients. The range is 1 to 8000.

Wireless Switch Channel and Power Commands

The commands in this section provide status and configuration for automatic channel planning and power adjustment.

channel-plan mode

This command configures the channel plan mode for each 802.11a/n and 802.11b/g/n frequency band. If it is `interval`, a channel plan is computed and applied at every defined interval. If it is `manual`, you must start and apply the channel plan manually. If it is `time`, then the channel plan will be computed and applied at the scheduled time.

Default manual

Format `channel-plan {an | bgn} mode {interval | manual | time}`

Mode Wireless Config

Parameter	*Description*
an	Configure channel plan mode for 802.11a/n.
bgn	Configure channel plan mode for 802.11b/g/n.
interval	Compute and apply new channel plans at the configured interval.
manual	Compute and apply new channel plans only when requested via the UI.
time	Compute and apply a new channel plan at the configured time.

channel-plan interval

This command configures the channel plan interval for each 802.11a/n and 802.11b/g frequency band. When the corresponding channel plan mode is configured for **interval**, this parameter indicates how often new channel plans are computed and applied.

Default 6

Format `channel-plan {an | bgn} interval hours`

Mode Wireless Config

Parameter	*Description*
an	Configure channel plan mode for 802.11a/n.
bgn	Configure channel plan mode for 802.11b/g/n.
`hours`	The channel plan interval in hours. The range is 6–24 hours.

no channel-plan interval

The `no` version of this command returns the configured channel plan interval to the default.

Format `no channel-plan {an | bgn} interval`

Mode Wireless Config

channel-plan time

This command configures the channel plan time for each 802.11a/n and 802.11b/g/n frequency band. When the corresponding channel plan mode is configured for time, this parameter indicates the time of day a new channel plan is computed and applied.

Default 00:00

Format `channel-plan {an | bgn} time hh:mm`

Mode Wireless Config

Parameter	*Description*
an	Configure channel plan mode for 802.11a/n.
bgn	Configure channel plan mode for 802.11b/g/n.
hh:mm	The channel plan time in 24 hour time.

Example: The following shows an example of the command.

```
Switch (Config wireless)# channel-plan an time 23:59 ?
<cr>    Press Enter to execute the command.
```

no channel-plan time

The no version of this command returns the configured channel plan time to the default.

Format `channel-plan {an | bgn} time`

Mode Wireless Config

channel-plan history-depth

This command configures the number of channel plan history iterations that are maintained for each 802.11a/n and 802.11b/g/n frequency band. The number of iterations stored for each channel plan affects channel assignment; the channel algorithm will not assign the same channel to an AP more than once within the number of stored iterations of the channel plan.

Default 5

Format `channel-plan {an | bgn} history-depth {0-10}`

Mode Wireless Config

Parameter	*Description*
an	Configure channel plan mode for 802.11a/n.
bgn	Configure channel plan mode for 802.11b/g/n.
0–10	Channel plan history depth.

no channel-plan history-depth

The no version of this command returns the history depth for the channel plan to the default.

Format `no channel-plan {an | bgn} history-depth`

Mode Wireless Config

power-plan mode

This command configures the power plan mode for managed APs. If it is `interval`, power adjustments are computed and applied at every defined interval. If it is `manual`, you must start and apply proposed power adjustments manually.

Default manual

Format `power-plan mode {interval | manual}`

Mode Wireless Config

Parameter	*Description*
interval	Compute and apply power adjustments at the configured interval.
manual	Compute and apply power adjustments only when requested via the UI.

power-plan interval

This command configures the power adjustment interval. When the power plan mode is configured for **interval**, this parameter indicates how often new power adjustments are computed and applied.

Default 4

Format `power plan interval {1-24}`

Mode Wireless Config

Parameter	*Description*
1–24	The power plan interval in hours.

no power-plan interval

The `no` version of this command returns the configured power adjustment interval to the default.

Format `no power-plan interval`

Mode Wireless Config

wireless channel-plan

This command allows you to request manual channel plan actions for each 802.11n and 802.11b/g/n frequency band.

Format `wireless channel-plan {an | bgn} [peer group] {apply | clear | start}`

Mode Privileged EXEC

Parameter	*Description*
an	Configure channel plan mode for 802.11a/n.
bgn	Configure channel plan mode for 802.11b/g/n.
peer group	Run the channel plan for the entire peer-group.
apply	Apply the entire proposed channel plan.
clear	Clear the current proposed channel plan.
start	Compute a new proposed channel plan.

wireless power-plan

This command allows you to manage manual power adjustments for the managed APs.

Format `wireless power-plan [peer group] {apply | clear | start}`

Mode Privileged EXEC

Parameter	*Description*
peer group	Run the power plan for the entire peer-group.
apply	Apply the proposed power adjustments.
clear	Clear the proposed power adjustments.
start	Compute new proposed power adjustments.

show wireless channel-plan

This command displays configuration for automatic channel planning. The channel plan type argument must be specified, the configuration and status is maintained separately for each radio frequency.

Format `show wireless channel-plan {an | bgn}`

Mode Privileged EXEC

Field	*Description*
an	Configure channel plan mode for 802.11a/n.
bgn	Configure channel plan mode for 802.11b/g/n.
Channel Plan	The channel plan type or mode, managed AP radios operating in the specified mode will be considered for this channel plan.
Channel Plan Mode	The frequency for automatic channel planning manual, fixed time, or interval. If the mode is manual, the channel algorithm will not run unless you request it.
Channel Plan Interval	If the channel plan mode is interval, this indicates the frequency in hours that the channel plan is computed and applied.
Channel Plan Fixed Time	If the channel plan mode is fixed time, this indicates the time (24-hour time) at which the channel plan is computed and applied.
Channel Plan History Depth	This indicates the number of iterations of the channel plan that are maintained in the channel plan history. The channel on a managed AP radio will not be changed more than once within the channel plan history.

show wireless channel-plan history

This command displays a history for the automatic channel algorithm. The channel plan type argument must be specified. A channel history is maintained separately for each radio frequency. The channel algorithm maintains a configured number of iterations of applied channel changes to avoid frequent channel changes to the same managed AP radio. If the IP address is not entered, the command displays a history summary for all peer switches. If a peer switch IP address is entered, detailed history for that peer switch is displayed.

Format `show wireless channel-plan history {an | bgn} [ipaddr]`

Mode Privileged EXEC

Field	*Description*
ipaddr	A valid IP address.
an	Configure channel plan mode for 802.11a/n.
bgn	Configure channel plan mode for 802.11b/g/n.
Current Iteration	Indicates the current iteration of the channel plan.
Operational Status	Indicates whether automatic channel planning is active or inactive. Automatic channel planning may be inactive due to 802.11h or unsupported clear channels.

Field	*Description*
Last Algorithm Time	Indicates the last time the channel planning algorithm completed.
AP MAC address	The managed AP Ethernet MAC address.
Location	A descriptive location string configured for the managed AP.
Radio	The radio interface on the managed AP.
Iteration	Iteration of the channel plan where the new channel was computed and applied.
Channel	The channel computed and applied to the managed AP.

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

```
(Switch) #show wireless channel-plan history a

Switch           Current        Last Algorithm
IP Address       Iteration      Time
--------------   --------       --------------
10.0.0.1         2              JAN 03 23:32:06 1970
10.254.22.1      3              JAN 03 23:33:06 1970
10.254.22.15     1              JAN 03 23:32:06 1970
10.254.22.16     0              --


Switch) #show wireless channel-plan history a 10.254.22.15
Switch IP Address.............................. 10.254.22.15
Current Iteration.............................. 0
Operational Status............................. Active

Last Algorithm Time...........................JAN 03 23:32:06 1970

AP MAC Address    Location             Radio  Iteration Channel
----------------- -------------------- ------ --------- -------
00:00:85:00:50:00 Third floor          1      1         6
```

show wireless channel-plan proposed

This command displays the proposed channel plan changes for a manual request to run the channel algorithm. The channel plan type argument must be specified. The channel algorithm is run separately for each radio frequency. The proposed channel changes may be cleared or applied using the **wireless channel-plan** command. If the IP address is not entered, the command displays a proposed summary for all peer switches. If a peer switch IP address is entered, detailed proposed entries for that peer switch are displayed.

Format `show wireless channel-plan proposed {an | bgn} [ipaddr]`

Mode Privileged EXEC

Field	*Description*
ipaddr	A valid IP address.
an	Configure channel plan mode for 802.11a/n.

Field	*Description*
bgn	Configure channel plan mode for 802.11b/g/n.
Current Status	Indicates the status of a manual channel plan request.
AP MAC Address	The managed AP Ethernet MAC address.
Location	A descriptive location string configured for the managed AP.
Radio	The radio interface on the managed AP.
Current Channel	The current channel on the managed AP radio.
New Channel	The new channel computed by the channel algorithm.

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

```
(Switch) #show wireless channel-plan proposed a


Switch IP Address       Current Status
------------------      ---------------
10.0.0.1                Apply Complete
10.254.22.1             Apply Complete
10.254.22.15            Apply Complete

(Switch) #show wireless channel-plan proposed a 10.254.22.15
Current Status.............................. Apply Complete

                                                    Current New
AP MAC Address   Location                   Radio Channel Channel
---------------- -------------------------- ----- ------- -------
00:00:85:00:50:00 Third floor                1     11      1
```

show wireless power-plan

This command displays status and configuration for automatic power adjustment. The command does not accept any arguments.

Format `show wireless power-plan`

Mode Privileged EXEC

Field	*Description*
Power Plan Mode	The mode for automatic power adjustment, manual or interval. If the mode is manual, the power algorithm will not run unless you request it.
Power Plan Interval	If the power adjustment mode is interval, this indicates the frequency in minutes that power adjustments are computed and applied.

show wireless power-plan proposed

This command displays the proposed power adjustments for a manual request to run the power algorithm. The command does not accept any arguments. The proposed power changes may be cleared or applied using the **wireless power-plan** command. If the IP address is not entered, the command displays a proposed summary for all peer switches. If a peer switch IP address is entered, detailed proposed entries for that peer switch are displayed.

Format `show wireless power-plan proposed [ipaddr]`

Mode Privileged EXEC

Field	*Description*
ipaddr	A valid IP address.
Current Status	Indicates the status of a manual power adjustment request.
AP MAC Address	The managed AP Ethernet MAC address.
Location	A descriptive location string configured for the managed AP.
Radio	The radio interface on the managed AP.
Current Power	The current transmit power on the managed AP radio.
New Power	The new transmit power computed by the power algorithm.

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

```
(Switch) #show wireless power-plan proposed
Switch IP Address  Current Status
-----------------  --------------
10.0.0.1           Algorithm Completed
10.254.22.1        Algorithm Completed
10.254.22.15       Algorithm Completed


(Switch) #show wireless power-plan proposed 10.254.22.15
Current Status.............................. Algorithm Complete
No proposed power adjustments to display.
```

Peer Wireless Switch Commands

The commands in this section provide peer Wireless Switch status.

show wireless peer-switch

This command displays status information for peer Wireless Switches. If no parameters are entered, the command will display summary status for all peer switches. If a peer switch IP address is entered, detailed status for that peer switch is displayed.

Format `show wireless peer-switch [ipaddr]`

Mode Privileged EXEC

Field	*Description*
ipaddr	A valid IP address.
IP Address	IP address of the peer switch.
Vendor ID	The peer switch software vendor ID.
Software Version	Version of WS software on the peer switch.
Protocol Version	Protocol version of WS software on the peer switch.
Discovery Reason	Method for peer WS discovery.
Managed AP Count	Total number of access points currently managed by the peer switch.
Age	Time since last update was received from the switch.

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

```
(Switch) #show wireless peer-switch

                Vendor   Software              Protocol  Discovery
IP Address      ID       Version               Version   Reason     Age
--------------  ------   -------------------   --------  ---------  -----------
10.0.0.1        Broadcom 1.1                   1         IP Poll    00h:01m:18s
10.254.22.1     Broadcom 1.1                   1         IP Poll    00h:01m:18s
10.254.22.15    0x0016   1.0                   1         IP Poll    00h:01m:18s

(Switch) #show wireless peer-switch 10.254.22.1

IP Address..................................... 10.254.22.1
Vendor ID...................................... Broadcom
Software Version............................... 1.1
Protocol Version............................... 1
Discovery Reason............................... IP Poll
Managed AP Count............................... 3
Age............................................ 0d:00:00:11
```

show wireless peer-switch configure status

This command displays config push status information for peer wireless switches. If no parameters are entered, the command will display summary status for all peer switches. If a peer switch IP address is entered, detailed status for that peer switch is displayed.

Format `show wireless peer-switch [ipaddr] configure status`

Mode Privileged EXEC

Field	*Description*
ipaddr	A valid IP address.
IP Address	The IP address of the peer switch.
Configuration Switch IP Address	The peer switch IP address last config received.
Configuration Status	Config push status from the Wireless Switch to this peer switch.
Configuration Received	Configuration groups received as part of config push from the peer switch.
Rx Time	The time the config push was received from the peer switch.

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

```
(Switch) #show wireless peer-switch configure status
                Configuration
IP Address      Switch IP Address   Configuration               Rx Time
--------------  ------  -------------------  --------  ---------  -----------
10.0.0.100      10.254.22.1        AP Database,AP Profile..  JAN 03 23:32:06 1970
10.0.0.101      10.254.22.1        AP Database,AP Profile..  JAN 03 23:32:06 1970
10.0.0.102      10.254.22.1        AP Profile,Channel..      JAN 03 23:32:06 1970

(Switch) #show wireless peer-switch 10.0.0.100 configure status

IP Address..................................... 10.0.0.100
Configuration Switch IP Address................ 10.254.22.1
Configuration Status........................... Failure Invalid Code Version
Configuration Received......................... AP Database,
                                                AP Profile,
                                                Channel Power,
                                                Discovery,
                                                Global,
                          Known-Client
Rx Time   ..................                  JAN 03 23:32:06 1970
```

show wireless peer-switch ap status

This command displays the operational status for a peer Wireless Switch-managed AP. If no parameters are specified, the command will display a summary of all Wireless Switch-managed APs. If an AP MAC address is specified, the detailed status is displayed.

Format `show wireless peer-switch [ipaddr] ap [macaddr] status`

Mode Privileged EXEC

Field	*Description*
ipaddr	A valid IP address.
macaddr	Wireless Switch-managed AP MAC address.
IP Address	The network IP address of the peer Wireless Switch-managed AP.
MAC Address	The Ethernet address of the peer Wireless Switch-managed AP.
Peer Switch IP Address	The network IP address of the peer Wireless Switch managing the AP.
Location	A location description for the AP, this is the value configured in the valid AP database (either locally or on the RADIUS server).
Profile	The AP profile configuration currently applied to the peer Wireless Switch-managed AP.
Hardware Type	Hardware platform for the AP, this is learned from the AP during discovery.

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

```
(Switch) #show wireless peer-switch ap status
                  Peer Switch
MAC Address       IP Address        Location       Profile        HwType
----------------- ---------------   ------------   -------------  -----------
00:01:01:02:01:01 192.168.0.100     Ground Floor   1-Default      Broadcom
00:01:01:02:02:01 192.168.0.100     Ground Floor   1-Default      Broadcom
00:01:01:02:03:0  192.168.0.200     Conf Room…     2-L3 Roaming.. Broadcom
00:01:01:02:04:01 192.168.0.300     First Floor    3-WPA2 VAPs..  Broadcom

(Switch) #
(Switch) #show wireless peer-switch 192.168.0.100 ap status
                  Peer Switch
MAC Address       IP Address     Location       Profile        HwType
----------------- -------------- ------------   -------------  -----------
00:01:01:02:01:01 192.168.0.100  Ground Floor   1-Default      Broadcom
00:01:01:02:02:01 192.168.0.100  Ground Floor   1-Default      Broadcom


(Switch) #show wireless peer-switch ap 00:01:01:02:02:01 status

MAC Address..................................... 00:01:01:02:01:01
Peer Switch IP Address.........................192.168.0.100
IP Address...................................... 192.168.0.1
Location........................................ Conf Room Bldg 200
Profile......................................... 2 – L3 Roaming Profile
Hardware Type................................... Broadcom
```

Local Access Point Database Commands

The commands in this section provide configuration of the local valid AP database. These configurations may also be performed on an external RADIUS server.

ap database

This command adds an AP to the local valid AP database (if not already present) and enters the AP configuration mode identified by the AP MAC address. In AP configuration mode, you can configure parameters for each individual valid AP. Note that if a valid AP is already being managed by the switch, you need to reset the AP to pick up any configuration changes in the valid AP database. The valid AP database parameters are read only when the AP is validated during discovery.

Format `ap database macaddr`

Mode Wireless Config

Parameter	*Description*
macaddr	MAC address of a physical AP.

no ap database

The no version of this command deletes the AP entry for the specified MAC address from the local database or all the entries present in the database.

Format `no ap database [macaddr]`

Mode Wireless Config

mode (AP Config Mode)

This command configures the managed mode for an AP.

Default ws-managed

Format `mode {ws-managed | standalone | rogue}`

Mode AP Config

Parameter	*Description*
ws-managed	AP is managed by the Wireless Switch upon discovery.
standalone	AP is managed as a standalone AP and should not be reported as rogue by the Wireless Switch.
rogue	AP is identified as an administrator-configured rogue AP and will be reported as rogue upon discovery.

location

This command configures a descriptive string for the AP location.

Format `location value`

Mode AP Config

Parameter	*Description*
value	This parameter is an AP location string. It should not be more than 32 characters long. To use spaces in the location, enclose the value with quotes, for example "Conference Room A".

no location

The `no` version of this command deletes the current location string for the AP.

Format `no location`

Mode AP Config

password (AP Config Mode)

This command configures the password that this AP must use to authenticate to the Wireless Switch. The password is only verified if global AP authentication is enabled. After you enter the password, the CLI prompts you to enter a password that is between 8–63 alphanumeric characters.

Default The default password is blank.

Format `password`

Mode AP Config

no password

The `no` version of this command deletes the password for the AP.

Format `no password`

Mode AP Config

Example: The following shows an example of the command.

```
Switch (Config-ap)# password ?
<cr>Press Enter to execute the command.

Switch (Config-ap)# password <cr>
Enter Password (8 - 63 characters):<enter here>
Re-enter password:<enter same here>

Switch (Config-ap)# no password <cr>
Switch (Config-ap)#
```

password encrypted

This command configures the password that this AP must use to authenticate to the Wireless Switch. The password is only verified if global AP authentication is enabled. The command accepts the AP password in an encrypted format.

Default The default password is blank.

Format `password encrypted password`

Mode AP Config

Parameter	*Description*
password	The password in encrypted format, 128 hexadecimal characters.

profile

This command configures the AP profile to be used to configure this AP. The profile configuration is used only if the AP mode is Wireless Switch-managed.

Default 1 - Default

Format `profile {1-16>}`

Mode AP Config

Parameter	*Description*
1–16	Indicates the AP profile ID for AP configuration.

no profile

The `no` version of this command sets the current profile ID for the AP to the default profile.

Format `no profile`

Mode AP Config

radio

This command allows you to configure fixed channel and/or power settings for a radio on the AP. If the channel is not valid for the physical mode configured within the AP configuration profile, this configuration is ignored.

Default channel 0 (auto), power 0 (auto)

Format `radio {1-2} {channel channel | power pwr-level}`

Mode AP Config

Parameter	*Description*
1–2	The radio interface on the AP.
channel	0 (auto) or a fixed channel for the radio. The valid range is based on the configured country code.
`pwr-level`	0 (auto) or a fixed transmit power for the radio ranging from 1–100. The value is entered as % of maximum power.

standalone channel (Stand-alone AP expected channel)

This command configures the expected channel for an AP in stand-alone mode.

Default 0 (any channel)

Format `standalone channel channel`

Mode AP Config

Parameter	*Description*
channel	A valid channel from 0 to 161 from the all-country aggregate channel list. Channel zero indicates that any valid channel is allowed.

no standalone channel

The `no` version of this command configures the expected channel for an AP in stand-alone mode to the default – any channel is allowed.

Format `no standalone channel`

Mode AP Config

standalone security (Stand-alone AP expected security mode)

This command configures the expected security mode for an AP in stand-alone mode.

Default any

Format `standalone security {any | open | wep | wpa}`

Mode AP Config

Parameter	*Description*
any	All security modes are allowed; open security, WEP and WPA/WPA2.
open	Only open security mode is allowed for the AP.
wep	Only WEP security is allowed for the AP.
wpa	Only WPA/WPA2 security is allowed for the AP.

no standalone security

The no version of this command configures the expected security mode for an AP in stand-alone mode to the default – any security mode is allowed.

Format `no standalone security`

Mode AP Config

standalone ssid (Stand-alone AP expected SSID)

This command configures the expected SSID for an AP in stand-alone mode.

Default " " (empty string – any SSID is allowed).

Format `standalone ssid name`

Mode AP Config

Parameter	*Description*
name	The service set ID must be between 1 and 32 characters. Use the no form of the command to configure the AP to operate on any SSID.

no standalone ssid

The no version of this command configures the expected SSID for an AP in stand-alone mode.

Format `no standalone ssid`

Mode AP Config

standalone wds-mode (Stand-alone AP expected WDS mode)

This command configures the expected WDS mode for an AP in stand-alone mode.

Default any

Format `standalone wds-mode {any | bridge | normal}`

Mode AP Config

Parameter	*Description*
any	Operation as a bridge or in normal mode is allowed.
bridge	Normal mode operation is not allowed. The stand-alone AP is expected to operate as a bridge.
normal	Operation as a bridge is not allowed.

no standalone wds-mode

The `no` version of this command configures the expected WDS mode for an AP in stand-alone mode to the default – any WDS mode is allowed.

show wireless ap database

This command displays the valid AP database entries. If no parameters are entered, a summary is displayed. You can enter a MAC address to display detailed information for a specific AP.

Format `show wireless ap database [macaddr]`

Mode Privileged EXEC

Field	*Description*
macaddr	The MAC Address corresponding to the AP's Ethernet interface.
Location	A description for the AP, often based on its location.
AP Mode	Indicates the configured mode of the AP is either `ws-managed`, `standalone`, or `rogue`.
Profile	This indicates the configuration profile. If the AP is in managed mode this is the profile sent to the AP.
Password Configured	If the authentication password is configured, the value displayed will be *Yes*, otherwise it will be *No*.
Radio 1 Channel	This indicates Auto or a fixed channel for radio 1.
Radio 2 Channel	This indicates Auto or a fixed channel for radio 2.
Radio 1 Transmit Power	This indicates Auto or a fixed power setting for radio 1.
Radio 2 Transmit Power	This indicates Auto or a fixed power setting for radio 2.

Field	*Description*
Standalone Expected Channel	Expected channel for stand-alone mode.
Standalone Expected Security Mode	Expected security for stand-alone mode.
Standalone Expected SSID	Expected SSID for stand-alone mode.
Standalone Expected WDS Mode	Expected WDS mode for stand-alone mode.

Example: The following shows example CLI display output for the command when an AP MAC address is specified.

```
(Switch) #show wireless ap database 11:33:44:55:66:77

AP MAC Address.............................. 11:33:44:55:66:77
Location.....................................
AP Mode..................................... ws-managed
Password Configured......................... No
Profile..................................... 1 - Default
Radio  1 Channel............................ Auto
Radio  1 Power.............................. Auto
Radio  2 Channel............................ Auto
Radio  2 Power.............................. Auto
Stand-alone Expected Channel................ 0
Stand-alone Expected Security Mode.......... Any
Stand-alone Expected SSID....................
Stand-alone Expected WDS Mode............... Any

(Switch) #show wireless ap-database
MAC Address           Location                          AP Mode
--------------------  --------------------------------  -------------
00:77:77:77:52:00     lab                               ws-managed
11:10:10:10:10:10     conference-room                   standalone
```

Wireless Network Commands

The commands in this section provide configuration of wireless networks.

network (Wireless Config Mode)

This command adds a network configuration (if not already present) and enters the network configuration mode. In this mode, you can modify the network configuration parameters.

Default Networks 1–16 are created by default.

Format `network {1-64}`

Mode Wireless Config

Parameter	*Description*
1–64	Integer ID for the network.

no network

The `no` version of this command deletes a configured network. If a network is applied to one or more VAPs within an AP profile, it cannot be deleted. The first sixteen default networks can never be deleted.

Format `no network`

Mode Wireless Config

ssid

This command configures the SSID for the wireless network. A network must be configured with an SSID of one or more characters. The SSID can be modified, but cannot be deleted. Except for the default Guest Network, the default SSID for each network is 'Managed SSID' followed by the unique Network ID.

Default Network 1 - Guest Network
Network *networkid* – Managed SSID *networkid*

Format `ssid name`

Mode Network Config

Parameter	*Description*
name	Service Set Identifier, must be between 1–32 alphanumeric characters. To use spaces in the SSID, use quotes around the name.

vlan (Network Config Mode)

This command configures the default VLAN ID for the network. If there is no RADIUS server configured or a client is not associated with a VLAN via RADIUS, this is the VLAN assigned.

Default 1 – Default VLAN

Format `vlan {1-4094}`

Mode Network Config

Parameter	*Description*
1–4094	A valid VLAN ID.

no vlan

The `no` version of this command sets the default VLAN ID for the network to its default value.

Format `no vlan`

Mode Network Config

hide-ssid

This command enables hiding of the SSID for this network. If enabled, the SSID is not included in the AP beacon frames.

Default Disable

Format `hide-ssid`

Mode Network Config

no hide-ssid

The `no` version of this command disables hiding of the SSID for this network.

Format `no hide-ssid`

Mode Network Config

client-qos access-control

This command configures the default access control list used by clients associated with this network that do not obtain their own value via RADIUS. The `acl-name` parameter is a case-sensitive alphanumeric string from 1 to 31 characters. The access list specified in this command must currently exist in the wireless switch. The `acl-id` parameter range is 1–199.

Format `client-qos access-control {down | up} {ip {acl-id | acl-name} | ipv6 acl-name | mac acl-name}`

Mode Network Config

no client-qos access-control

The `no` version of this command removes the client QoS default access control list parameter configured for this network.

Format `no client-qos access-control {down | up}`

Mode Network Config

client-qos bandwidth-limit

This command configures the default maximum bandwidth rate limit in bits per second used by clients associated with this network that do not obtain their own value via RADIUS.

Note: The specified value is subject to rounding down to the nearest 64000 in the AP, with a minimum rounded value of 64000.

Format `client-qos bandwidth-limit {down | up} {1-4294967295}`

Mode Network Config

no client-qos bandwidth-limit

The `no` version of this command sets the client QoS default maximum bandwidth rate limit parameter to 0 for this network, disabling rate limiting for clients that associate with this network and use this default value.

Format `no client-qos bandwidth-limit {down | up}`

Mode Network Config

client-qos diffserv-policy

This command configures the default Diffserv policy used by clients associated with this network that do not obtain their own value via RADIUS. The `policy-name` parameter is a case-sensitive alphanumeric string from 1 to 31 characters and must specify a Diffserv policy that currently exists in the wireless switch.

Format `client-qos diffserv-policy {down | up} policy-name`

Mode Network Config

no client-qos diffserv-policy

The `no` version of this command removes the client QoS default Diffserv policy parameter configured for this network.

Format `no client-qos diffserv-policy {down | up}`

Mode Network Config

client-qos enable

This command enables AP client QoS operation for the network. When enabled, and when the wireless global client QoS mode is also enabled, clients associated to this network may have one or more of the following QoS facilities in effect in the down and/or up directions: access control, bandwidth limiting, and Differentiated services (via policy).

Default `Disable`

Format `client-qos enable`

Mode Network Config

no client-qos enable

The `no` version of this command disables AP client QoS operation for the network. Client traffic is not subject to QoS processing for any clients attached to this wireless network.

Format `no client-qos enable`

Mode Network Config

deny-broadcast

This command enables deny broadcast mode for the network. This means the AP will not respond to client probe requests broadcast to all available SSIDs.

Default Disable

Format `deny-broadcast`

Mode Network Config

no deny-broadcast

The no version of this command disables deny broadcast mode for the network. This means the AP will respond to client probe requests for all available SSIDs.

Format `no deny-broadcast`

Mode Network Config

redirect mode

This command enables and configures the mode for redirection of wireless client traffic on this network. If HTTP redirection is enabled, initial client requests are redirected to the configured URL. If IP redirection is enabled, all client requests are redirected to the configured IP address.

Default None

Format `redirect mode {http | ip}`

Mode Network Config

no redirect mode

The no version of this command disables redirect on the network.

Format `no redirect mode`

Mode Network Config

redirect url

This command configures a URL for HTTP redirection. When HTTP redirection is enabled on the network, each initial client request is directed to this URL. Note that http:// is not entered in the configured URL because this prefix is assumed.

Default None (The default is blank.)

Format `redirect url url`

Mode Network Config

Parameter	*Description*
url	A Uniform Resource Locator, for example www.cnn.com. The URL must be 0–128 characters.

no redirect url

The no version of this command removes the configured URL. The value is set to an empty string.

Format `no redirect url`

Mode Network Config

security mode

This command configures the authentication and encryption mode on the network.

Default none

Format `security mode {none | static-wep | wep-dot1x | wpa-enterprise | wpa-personal}`

Mode Network Config

Parameter	*Description*
none	No authentication or encryption on the network.
static-wep	Static WEP encryption, authentication is configured separately.
wep-dot1x	Dynamic WEP authentication using 802.1x.
wpa-enterprise	WPA 802.1x authentication.
wpa-personal	WPA shared-key authentication.

no security mode

The `no` version of this command sets the security mode to its default value.

Format `no security mode`

Mode Network Config

wep authentication

This command configures the static WEP authentication mode for the network. This value is applicable only when the security mode is configured for static WEP authentication and encryption.

Default Open System

Format `wep authentication {open-system [shared-key] | shared-key}`

Mode Network Config

Parameter	*Description*
open system	No authentication required.
shared-key	Clients are required to authenticate to the network using a shared key.

no wep authentication

The no version of this command sets WEP authentication mode to the default value, which is **open system**.

Format `no wep authentication`

Mode Network Config

wep key

This command configures up to 4 static WEP keys for the network. The configured keys are used when the network security mode is set to WEP shared key, according to the configured WEP transfer key index. The number of characters required depends on the configured WEP key type and length.

Format `wep key {1-4} value`

Mode Network Config

Parameter	*Description*
1–4	A valid WEP key index.
value	The WEP key itself, entered in ASCII or HEX format. The following list shows the number of keys to enter in the field: • 64 bit —ASCII: 5 characters; Hex: 10 characters • 128 bit —ASCII: 13 characters; Hex: 26 characters • 152 bit —ASCII: 16 characters; Hex: 32 characters. For more information, please see the “Static WEP” table in the *DWS-4000 User Manual*.

no wep key

The no version of this command removes the corresponding WEP key configuration.

Format `no wep key {1-4}`

Mode Network Config

wep tx-key

This command configures the WEP key index to be used for encryption on the network. This value is applicable only when the security mode is configured for WEP shared key authentication and encryption.

Default 1

Format `wep tx-key {1-4}`

Mode Network Config

Parameter	*Description*
1–4	A valid WEP key index value.

no wep tx-key

The `no` version of this command sets the WEP transmit key index to its default value.

Format `no wep tx-key`

Mode Network Config

wep key type

This command configures the WEP key type for the network. The configured key type is used when the network security mode is set to WEP shared key. The WEP key type affects the number of characters required for a valid WEP key, and therefore changing the WEP key length will reset all keys.

Default ASCII

Format `wep key type {ascii | hex}`

Mode Network Config

Parameter	*Description*
ascii	Set WEP key type to ASCII.
hex	Set WEP key type to hexadecimal.

no wep key type

The `no` version of this command returns the WEP key type to its default value.

Format `no wep key type`

Mode Network Config

wep key length

This command configures the WEP key length in bits for the network. The configured key length is used when the network security mode is set to WEP shared key. The WEP key length affects the number of characters required for a valid WEP key, and therefore changing the WEP key length will reset all keys.

Default 128

Format `wep key length {64 | 128}`

Mode Network Config

no wep key length

The no version of this command returns the WEP key length to its default value.

Format `no wep key length`

Mode Network Config

mac authentication

This command enables and configures the mode for client MAC authentication on the network.

Default Disable

Format `mac authentication {local | radius}`

Mode Network Config

Parameter	*Description*
local	Enable MAC authentication using the AP profile MAC authentication list.
radius	Enable MAC authentication using the configured RADIUS server.

no mac authentication

The no version of this command disables MAC authentication on the network.

Format `no mac authentication`

Mode Network Config

radius server-name

This command configures the RADIUS authentication/accounting server name for wireless clients authenticating to this network. The server name can contain alphanumeric characters plus –, _, and space.

Default Default-RADIUS-Server – authentication server name
Default-RADIUS-Server – accounting server name

Format `radius server–name {auth | acct} name`

Mode Network Config

Parameter	*Description*
name	Enter an alphanumeric string up to 32 characters in length.

no radius server-name

The no version of this command sets the RADIUS authentication/accounting server name to the default value.

Format `no radius server–name {auth | acct}`

Mode Network Config

Example: The following shows an example of the command.

```
(Switch) #radius server-name auth  “Wireless_Network-1 Auth_Server 1” ?
<cr>    Press Enter to execute the command.

(Switch) #no radius server-name auth ?
<cr>    Press Enter to execute the command.

(Switch) #radius server-name acct  “Wireless_Network-1 Acct_Server 1” ?
<cr>    Press Enter to execute the command.

(Switch) #no radius server-name acct  ?
<cr>    Press Enter to execute the command.
```

radius use–network–configuration

This command configures the system to use the network RADIUS configuration for wireless client’s authentication on this network or to use global RADIUS configuration.

Default `Enable`

Format `radius use–network–configuration`

Mode Network Config

no radius use–network–configuration

The no version of this command configures the system to use the network RADIUS configuration for authentication of wireless clients on this network.

Format no radius use–network–configuration

Mode Network Config

Example: The following shows an example of the command.

```
(Switch) # radius use-network-configuration ?
<cr>Press Enter to execute the command.

(Switch) # no radius use-network-configuration ?
<cr>Press Enter to execute the command.
```

wpa versions

This command configures the WPA version(s) supported on the network. One or both parameters must be specified. This configuration only applies when the configured security mode is **WPA**.

Default wpa/wpa2

Format wpa versions {wpa [wpa2] | wpa2}

Mode Network Config

Parameter	*Description*
wpa	WPA version allowed.
wpa2	WPA2 version allowed.

no wpa versions

The no version of this command configures the supported WPA versions to the default value.

Format no wpa versions

Mode Network Config

wpa ciphers

This command configures the WPA cipher suites supported on the network; one or both parameters must be specified. This configuration only applies when the configured security mode is **WPA**.

Default tkip

Format `wpa ciphers {ccmp [tkip] | tkip}`

Mode Network Config

Parameter	*Description*
tkip	TKIP encryption.
ccmp	CCMP encryption.

no wpa ciphers

The `no` version of this command WPA returns supported cipher suites to the default value.

Format `no wpa ciphers`

Mode Network Config

wpa key

This command configures the WPA shared key. This is an alphanumeric string in the range 8-64 characters. The configured key is used when the network security mode is set to WPA shared key.

Default None

Format `wpa key value`

Mode Network Config

tunnel

This command enables client traffic tunneling on the network. For the tunnel to be operational, global routing must be enabled on the switch and the tunnel subnet, and mask must be configured and match a valid routing interface.

Default Disable

Format `tunnel`

Mode Network Config

no tunnel

The `no` version of this command disables client traffic tunneling on the network.

Format `no tunnel`

Mode Network Config

tunnel subnet

This command configures the tunnel subnet IP address for the network. This must match a configured routing interface in order for the tunnel to be operational.

Default Subnet IP - None
Subnet mask - 255.255.255.0

Format `tunnel subnet ipaddr [mask mask]`

Mode Network Config

Parameter	*Description*
ipaddr	A valid IP address.
mask	A valid subnet mask.

no tunnel subnet

The `no` version of this command deletes the configured tunnel subnet parameters.

Format `no tunnel subnet`

Mode Network Config

arp-suppression

This command enables wireless ARP suppression on the network. Enabling wireless ARP suppression allows for limiting ARP broadcasts on the wireless medium for IPv4 networks.

Default Disable

Format `arp-suppression`

Mode Network Config Mode

no arp-suppression

The `no` version of this command disables wireless ARP suppression on the network.

Format `no arp-suppression`

Mode Network Config Mode

wpa2 pre-authentication

This command enables WPA2 pre-authentication support for client roaming.

Default Enable

Format `wpa2 pre-authentication`

Mode Network Config

no wpa2 pre-authentication

The `no` version of this command disables WPA2 pre-authentication support.

Format `no wpa2 pre-authentication`

Mode Network Config

wpa2 pre-authentication limit

This command configures the WPA2 pre-authentication limit for the network. This specifies a limit on the number of APs within the peer group to which one client is allowed to pre-authenticate.

Default 0, no limit

Format `wpa2 pre-authentication limit {0-192}`

Mode Network Config

Parameter	*Description*
0–192	Valid WPA2 pre-authentication limit.

no wpa2 pre-authentication limit

The `no` version of this command sets the configured WPA2 pre-authentication limit to its default value.

Format `no wpa2 pre-authentication limit`

Mode Network Config

wpa2 key-forwarding

This command enables WPA2 key forwarding support for client roaming on the network.

Default Enable

Format `wpa2 key-forwarding`

Mode Network Config

no wpa2 key-forwarding

The no version of this command disables WPA2 key forwarding support on the network.

Format no wpa2 key-forwarding

Mode Network Config

wpa2 key-caching holdtime

This command configures the length of time a PMK will be cached by an AP for either client roaming or key forwarding.

Default 10

Format wpa2 key-caching holdtime {0-1440}

Mode Network Config

Parameter	*Description*
0–1440	WPA2 key caching hold time in minutes.

no wpa2 key-caching holdtime

The no version of this command sets the WPA2 key caching hold time to its default value.

Format no wpa2 key-caching holdtime

Mode Network Config

dot1x bcast-key-refresh-rate

This command specifies the interval after which the broadcast keys are changed.

Default 300 seconds

Format `dot1x bcast-key-refresh-rate {0-86400}`

Mode Network Config

Parameter	*Description*
0–86400	The bcast-key-refresh-rate range is 0 to 86400 in seconds.

no dot1x bcast-key-refresh-rate

The no version of this command returns the bcast-key-refresh-rate to its default value.

Format `no dot1x bcast-key-refresh-rate`

Mode Network Config

dot1x session-key-refresh-rate

This command specifies the interval after which the Unicast session keys are changed.

Default 0 seconds

Format `dot1x session-key-refresh-rate {0-86400}`

Mode Network Config

Parameter	*Description*
0–86400	The session-key-refresh-rate range is 0 to 86400 in seconds.

no dot1x session-key-refresh-rate

The no version of this command returns the session-key-refresh-rate to its default value.

Format `no dot1x session-key-refresh-rate`

Mode Network Config

clear (Network Config Mode)

This command restores a network configuration to default values.

Format `clear`

Mode Network Config

show wireless network

This command displays the network configuration parameters. If no parameters are specified, a summary of the configured networks is displayed, otherwise the detailed configuration is displayed.

Format `show wireless network [{1-64}]`

Mode Privileged EXEC

Field	*Description*
SSID	Service Set Identifier.
Interface ID	Internal interface number for this network.
Default VLAN	Default VLAN for the network.
Hide SSID	Indicates if SSID inclusion is suppressed from the beacons.
Deny Broadcast	Indicates if probe requests with broadcast SSID are denied on the network.
Redirect Mode	Indicates the mode of client traffic redirection.
Redirect URL	Indicates the configured URL for client HTTP redirection.
L2 Distributed Tunneling Mode	Indicates whether L2 distributed tunneling mode is enabled on the switch.
Bcast Key Refresh Rate	The interval after which the broadcast keys are changed.
Session Key Refresh Rate	the interval after which the Unicast session keys are changed
L3 Tunnel Mode	If tunneling feature is enabled, indicates if L3 roaming is enabled on the network.
L3 Tunnel Status	Indicates the if the tunnel is up or down.
L3 Tunnel Subnet IP	If tunneling feature is enabled, indicates the subnet for the tunnel.
L3 Tunnel Subnet Mask	If tunneling feature is enabled, indicates the network mask for the tunnel subnet.
Wireless ARP Suppression	Indicates whether wireless ARP suppression is enabled or disabled.
Security Mode	Indicates the authentication and encryption mode.
MAC Authentication	The client MAC address authentication mode.
RADIUS Authentication Server Name	RADIUS server name for authentication.
RADIUS Authentication Server Configured	Indicates whether the specified named RADIUS Authentication server is configured in the RADIUS Client configuration.
RADIUS Accounting Server Name	RADIUS server name for accounting.

Field	*Description*
RADIUS Accounting Server Configured	Indicates whether the specified named RADIUS Accounting server is configured in the RADIUS Client configuration.
WPA Versions	Indicates the WPA versions allowed when the WPA encryption mode is enabled.
WPA Ciphers	Indicates the encryption solutions to use when the WPA encryption mode is enabled.
WPA Key Type	Specifies the type of the WPA key configured (ASCII only).
Passphrase	The WPA passphrase
WPA2 Pre-Authentication Mode	If WPA2 encryption is enabled, indicates pre-authentication support for roaming WPA2 clients.
WPA2 Pre-Authentication Limit	If WPA2 pre-authentication is enabled, specifies a limit on the number of APs within the peer group to which one client is allowed to pre-authenticate.
WPA2 Key Caching Holdtime	Length of time in minutes that a PMK will be cached by an AP after the client using this PMK has roamed away from this AP.
WEP Authentication Type	Indicates whether Open System authentication or Shared Key authentication is used.
WEP Key Type	indicates whether the key is in hexadecimal format or ASCII text format.
WEP Key Length	If WEP – Shared Key security mode is enabled, specifies number of bits for the WEP Keys.
WEP Transfer Key Index	If WEP – Shared Key security mode is enabled, indicates which WEP key will be used for encryption.
WEP Key1–4	If WEP – Shared Key security mode is enabled, indicates the WEP keys configured for encryption. Up to 4 keys can be configured.
Client QoS Mode	Indicates whether client QoS operation is enabled on this network.
Client QoS Bandwidth Limit Down	Defines the default maximum rate limit in bits per second for traffic flowing from the AP to the client. A value of 0 disables rate limiting in this direction. This default is used for clients that do not obtain their own value via RADIUS.
Client QoS Bandwidth Limit Up	Defines the default maximum rate limit in bits per second for traffic flowing from the client to the AP. A value of 0 disables rate limiting in this direction. This default is used for clients that do not obtain their own value via RADIUS.
Client QoS Access Control Down	Defines the default access control list to use for traffic flowing from the AP to the client. Both the ACL type and its name (or number) is displayed. This default is used for clients that do not obtain their own value via RADIUS.
Client QoS Access Control Up	Defines the default access control list to use for traffic flowing from the client to the AP. Both the ACL type and its name (or number) is displayed. This default is used for clients that do not obtain their own value via RADIUS.
Client QoS Diffserv Policy Down	Defines the default Diffserv policy to use for traffic flowing from the AP to the client. This default is used for clients that do not obtain their own value via RADIUS.
Client QoS Diffserv Policy Up	Defines the default Diffserv policy to use for traffic flowing from the client to the AP. This default is used for clients that do not obtain their own value via RADIUS.

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

```
(Switch) #show wireless network

Network  SSID                              Hide SSID  Security Mode
```

```
-------  -------------------------------  ---------  -------------
1        Guest Network                    Disable    Open System
2        Managed SSID 2                   Disable    Dynamic WPA
3        Managed SSID 3                   Disable    Open System
4        Managed SSID 4                   Disable    Open System
5        Managed SSID 5                   Disable    Open System
6        Managed SSID 6                   Disable    Open System
7        Managed SSID 7                   Disable    Open System
8        Managed SSID 8                   Disable    Open System

(Switch) #show wireless network 3

SSID..................................... Managed SSID 3
Interface ID............................. 264
Default VLAN............................. 1
Hide SSID................................ Disable
Deny Broadcast........................... Disable
Redirect Mode............................ IP
Redirect URL............................. -----
L2 Distributed Tunneling Mode............ Disable
Bcast Key Refresh Rate................... 300
Session Key Refresh Rate................. 0
L3 Tunnel Mode........................... Disable
L3 Tunnel Status......................... None
L3 Tunnel Subnet IP...................... 0.0.0.0
L3 Tunnel Subnet Mask.................... 255.255.255.0
Wireless ARP Suppression................. Disable
Security Mode............................ None
MAC Authentication....................... Disable
RADIUS Authentication Server Name........ Default-RADIUS-Server
RADIUS Authentication Server Status...... Not Configured
RADIUS Accounting Server Name............ Default-RADIUS-Server
RADIUS Accounting Server Status.......... Not Configured
WPA Versions............................. WPA/WPA2
WPA Ciphers.............................. TKIP/CCMP
WPA Key Type............................. ASCII
Passphrase.............................
WPA2 Pre-Authentication.................. Enable
WPA2 Pre-Authentication Limit............ 0
WPA2 Key Caching Holdtime (minutes)...... 10
WEP Authentication Type.................. Open System
WEP Key Type............................. HEX
WEP Key Length (bits).................... 128
WEP Transfer Key Index................... 1
WEP Key 1.............................
WEP Key 2.............................
WEP Key 3.............................
WEP Key 4.............................
Client QoS Mode.......................... Disable
Client QoS Bandwidth Limit Down.......... 0
Client QoS Bandwidth Limit Up............ 0
Client QoS Access Control Down........... -----
Client QoS Access Control Up............. -----
Client QoS Diffserv Policy Down.......... -----
--More-- or (q)uit
Client QoS Diffserv Policy Up............ -----
```

Access Point Profile Commands

The commands in this section provide configuration of access point profiles. Access point profiles can be applied to multiple physical APs.

ap profile

This command adds an AP profile (if not already present) and enters the AP profile configuration mode. In this mode, you can modify the profile configuration parameters. You can modify an AP profile at any time. If the profile is associated with one or more Managed APs, you must use the `wireless ap profile apply` command to send the changes to those APs.

Default 1 - Default

Format `ap profile {1-16}`

Mode Wireless Config

Parameter	*Description*
1–16	Identifier for the AP Profile.

no ap profile

The `no` version of this command deletes a configured AP profile. If the profile is referenced by an entry in the valid AP database, or is applied to one or more managed APs, it cannot be deleted. The default profile (1 – Default) can never be deleted.

Format `no ap profile {1-16}`

Mode Wireless Config

Example: The following shows an example of the command.

```
Switch (Config-wireless)# ap profile 1
Switch (Config-ap-profile)#
```

If the profile is in use:

```
Switch (Config-wireless)# no ap profile 2
One or more managed APs are configured with this profile, it cannot be deleted.
```

name

This command allows you to configure a descriptive name for the AP Profile.

Default Default (AP profile 1)

Format `name name`

Mode AP Profile Config

Parameter	*Description*
name	AP Profile name; it must be less than 32 characters. Use quotes around a name that contains spaces.

no name

The `no` version of this command deletes the configured name for the AP profile.

Format `no name`

Mode AP Profile Config

hwtype

This command allows you to configure the AP hardware type. If the hardware type is 0, the profile can be applied to any managed AP irrespective of its hardware type. If the hardware type is a non-zero value, this AP profile is applied to only AP's matching configured hardware type.

Default 0

Format `hwtype {1-6}`

Mode AP Profile Config

Parameter	*Description*
1–6	AP hardware type.

no hwtype

This command allows you to set the AP hardware type to the default value.

Format `no hwtype`

Mode AP Profile Config

Example: The following shows an example of the command.

```
Switch (Config-ap-profile)#  no hwtype ?
<cr>    Press Enter to execute the command.
```

vlan (AP Profile Config Mode)

This command allows you to configure the VLAN ID used to send tracer packets by wired network detection algorithm. If VLAN is 0, the tracer packets will be sent untagged.

Default 1

Format `vlan {0-4094}`

Mode AP Profile Config

Parameter	*Description*
0–4094	Wired network detection VLAN ID.

Example: The following shows an example of the command.

```
Switch (Config-ap-profile)#  vlan 10 ?
<cr>    Press Enter to execute the command.
```

no vlan (AP Profile Config Mode)

This command allows you to set the wired network detection VLAN ID to the default value.

Format `no vlan`

Mode AP Profile Config

Example: The following shows an example of the command.

```
Switch (Config-ap-profile)#  no vlan
<cr>    Press Enter to execute the command.
```

ap profile copy

This command copies an entire existing AP profile to another profile. If the destination profile does not exist, it will be created.

Format `ap profile copy {1-16} {1-16}`

Mode Wireless Config

Parameter	*Description*
1–16	Source AP Profile ID.
1–16	Destination AP Profile ID.

Example: The following shows an example of the command.

If the destination AP Profile is associated with Managed APs:

```
Switch (Config-wireless)# ap profile copy 1 2 <cr>
The destination profile is associated with WS Managed APs. Do you want to overwrite the existing
profile (y/n)? <enter ‘y’ or ‘n’>
```

wireless ap profile apply

This command requests for the switch to resend the AP profile configuration to all managed APs associated with the profile. This allows you to apply configuration changes to the APs that are already managed.

Format `wireless ap profile apply {1-16}`

Mode Privileged EXEC

Parameter	*Description*
1–16	AP Profile ID.

Example: The following shows an example of the command.

If the profile is associated with WS Managed APs:

```
Switch (Config-wireless)# ap profile apply 1 <cr>
Do you want to apply the configuration to all managed APs associated with this profile? (y/n)
```

clear (AP Profile Config Mode)

This command restores an AP profile configuration to default values except for the profile name. The profile name is not an AP configuration and is only used for descriptive purposes, therefore it is not cleared with this command. To delete a profile name, use the **no name** command.

Format `clear`

Mode AP Profile Config

Example: The following shows an example of the command.

```
Switch (Config-ap-profile)# clear

All configurations will be set to the default values for this profile except the
profile name. Are you sure you want to clear the profile configuration? (y/n) y
```

show wireless ap profile

This command displays the configured AP profiles. If you do not enter any command parameters, a summary of all AP profiles is displayed. You can enter an AP profile ID to display detailed configuration for a specific profile.

Format `show wireless ap profile [{1-16} [radio [{1-2}]]]`

Mode Privileged EXEC

Field	*Description*
AP Profile ID	Existing AP profile ID.
Profile Name	A descriptive name for the corresponding AP profile ID.
Hardware Type	Existing AP hardware type ID and description string.
Wired Network Detection VLAN ID	The VLAND ID used for sending tracer packets by the wired network detection algorithm. A configured value of 0 results in the transmission of untagged tracer packets.
Profile Status	Indicates the current AP profile status: • **Configured**—the profile exists, no managed APs are configured with the profile. • **Associated**—one or more managed APs are configured with the profile. • **Apply Requested**—you have invoked the `apply` command for the profile. • **Apply In Progress**—the profile is currently being applied to the associated managed APs. When the **apply** is complete, the profile returns to **Associated** status.

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

```
(Switch) #show wireless ap profile 1

AP Profile ID.............................. 1
Profile Name............................... Default
Hardware Type..............................  0 – Any
Wired Network Detection Vlan ID.............  0 - Any
Profile Status............................. Configured
Valid APs Configured....................... 0
Managed APs Configured..................... 2
```

Access Point Profile RF Commands

The commands in this section provide RF configuration per radio interface within an access point profile.

radio

This command enters the AP profile radio configuration mode. In this mode you can modify the radio configuration parameters for an AP profile.

Format `radio {1-2}`

Mode AP Profile Config

Parameter	*Description*
1–2	The radio interface within the AP profile.

enable (AP Profile Radio Config Mode)

This command configures the administrative mode of the radio interface to the *on* state.

Default on

Format `enable`

Mode AP Profile Radio Config

no enable

The `no` version of this command configures the administrative mode of the radio interface to the *off* state.

Format `no enable`

Mode AP Profile Radio Config

mode (AP Profile Radio Config Mode)

This command configures the physical layer technology to use on the radio.

Default Radio 1, bgn
Radio 2, an

Format `mode {a | bg | an | bgn | n-only-a | n-only-g}`

Mode AP Profile Radio Config

Parameter	*Description*
a	Indicates 802.11a as physical mode.
bg	Indicates 802.11bg as physical mode.
an	Indicates 802.11a/n as physical mode.
bgn	Indicates 802.11b/g/n as physical mode. Only applicable for radio 2.
n-only-a	Indicates 802.11n in 5GHz band as physical mode. Only applicable for radio 1.
n-only-g	Indicates 802.11n in 2.4GHz band as physical mode. Only applicable for radio 2.

If the user attempts to change the radio mode to one that is not applicable to that radio, then the following error displays:

```
(Switch) (Config-ap-profile)#radio 1
(Switch) (Config-ap-radio)#mode bg
Failed to set physical mode for radio interface.
```

no mode (AP Profile Radio Config Mode)

The no version of this command is used to return the configured radio mode to the default.

Format `no mode`

Mode AP Profile Radio Config

rf-scan other-channels

This command enables the radio to perform RF scanning on channels other than its operating channel. The optional interval parameter indicates how often the radio leaves its operational channel.

Default
- Enabled
- interval, 60 seconds

Format `rf-scan other-channels [interval {30-120}]`

Mode AP Profile Radio Config

Parameter	*Description*
interval	Interval at which the AP will move away from its operating channel.
30–120	Time interval in seconds.

no rf-scan other-channels

The no version of this command disables scanning on other channels; the radio will always scan on its operational channel.

Format `no rf-scan other-channels`

Mode AP Profile Radio Config

rf-scan sentry

This command enables dedicated RF scanning and disables normal operation of the radio. The radio will not allow any client associations when sentry mode is enabled.

Default
- Disabled
- Channels, all

Format `rf-scan sentry [channels {a | bg | all}]`

Mode AP Profile Radio Config

Parameter	*Description*
channels	Indicates to scan channels within specified mode/frequency.
a	Perform RF scan on all 802.11a channels (5 GHz frequency).
bg	Perform RF scan on all 802.11b/g channels (2.4 GHz frequency).
all	Perform RF scan on all channels.

no rf-scan sentry

The `no` version of this command disables dedicated scanning and enables normal operation of the radio.

Format `no rf-scan sentry`

Mode AP Profile Radio Config

rf-scan duration

This command configures the RF scan duration for the radio. The duration indicates how long the radio will scan on one channel.

Default 10 milliseconds

Format `rf-scan duration {10-2000}`

Mode AP Profile Radio Config

Parameter	*Description*
10–2000	Time duration in milliseconds.

no rf-scan duration

The `no` version of this command returns the configured RF scan duration to its default value.

Format `no rf-scan duration`

Mode AP Profile Radio Config

station-isolation

This command enables the Station Isolation mode on the radio. When Station Isolation is enabled, the access point blocks communication between wireless clients. The access point still allows data traffic between its wireless clients and wired devices on the network, but not among wireless clients.

Default Disabled

Format `station-isolation`

Mode AP Profile Radio Config

no station-isolation

The `no` version of this command disables the station isolation mode on the radio.

Format `no station-isolation`

Mode AP Profile Radio Config

rate-limit

This command is used to enable broadcast and multicast traffic rate limiting on the radio. If no optional parameters are entered, the command enables rate limiting on the radio with the default values.

Default
- rate-limit, Disabled
- rate-limit normal, 50 packets per second
- rate-limit burst, 75 packets per second

Format `rate-limit [{normal {1-50} | burst {1-75}}]`

Mode AP Profile Radio Config

Parameter	*Description*
normal	Configures the rate limit for normal traffic; all traffic below this limit is transmitted.
burst	Configures the burst traffic rate. Traffic can occur in bursts up to this value before all traffic is considered to exceed the limit.

no rate-limit

The no version of this command is used to either disable broadcast/multicast traffic rate limiting, or to return the configured rate limits to the default values. If no parameters are entered, rate limiting is disabled on the radio. If the optional normal or burst parameters are entered, the specified rate is set to its default value.

Format `no rate-limit [{normal | burst }]`

Mode AP Profile Radio Config

beacon-interval

The command configures the beacon interval for the radio. The beacon interval indicates the interval at which the AP radio transmits beacon frames.

Default 100 milliseconds

Format `beacon-interval {20-2000}`

Mode AP Profile Radio Config

Parameter	*Description*
20–2000	Time interval in milliseconds at which the radio sends beacon frames.

no beacon-interval

The no version of this command configures the beacon interval to the default value.

Format `no beacon-interval`

Mode AP Profile Radio Config

dtim-period

The command configures the DTIM period for the radio. The DTIM period is the number of beacons between DTIMs. A DTIM is Delivery Traffic Indication Map which indicates there is buffered broadcast or multicast traffic on the AP.

Default 10 Beacons

Format `dtim-period {1-255}`

Mode AP Profile Radio Config

Parameter	*Description*
1–255	Number of beacons between DTIMs.

no dtim-period

The `no` version of this command configures the DTIM period to the default value.

Format `no dtim-period`

Mode AP Profile Radio Config

fragmentation-threshold

This command configures the fragmentation threshold for the radio. The fragmentation threshold indicates a limit on the size of packets that can be fragmented. A threshold of *2346* indicates there should be no fragmentation.

Default 2346 (no fragmentation)

Format `fragmentation-threshold {256-2346}`

Mode AP Profile Radio Config

Parameter	*Description*
256–2346	Fragmentation threshold for the radio, even values.

no fragmentation-threshold

The `no` version of this command configures the fragmentation threshold to the default value.

Format `no fragmentation-threshold`

Mode AP Profile Radio Config

rts-threshold

This command configures the RTS threshold for the radio. This indicates the number of octets in an MPDU, below which an RTS/CTS handshake shall not be performed.

Default 2347

Format `rts-threshold {0-2347}`

Mode AP Profile Radio Config

Parameter	*Description*
0–2347	RTS threshold for the radio.

no rts-threshold

The `no` version of this command configures the RTS threshold to the default value.

Format `no rts-threshold`

Mode AP Profile Radio Config

max-clients

This command configures the maximum number of simultaneous client associations allowed on the radio interface**.**

Default 256

Format `max-clients {0-256}`

Mode AP Profile Radio Config

Parameter	*Description*
0–256	Maximum number of simultaneous associations allowed on the radio interface.

no max-clients

The `no` version of this command configures the maximum number of simultaneous client associations allowed on the radio interface to the default value.

Format `no max-clients`

Mode AP Profile Radio Config

channel auto

This command enables auto channel adjustment for the radio. This indicates the initial AP channel assignment can be automatically adjusted by the switch.

Default Disabled

Format `channel auto`

Mode AP Profile Radio Config

no channel auto

The `no` version of this command without any parameters disables auto channel adjustment for the radio.

Format `no channel auto`

Mode AP Profile Radio Config

channel auto-eligible

This command enables either one or all of the supported channels on the radio to be eligible for auto-channel selection. If you specify one channel, the command will succeed *only if* this channel is supported by the current mode of the radio (use `show wireless ap profile profile-id radio radio-id auto-eligible` for valid values). If you supply `all` as the argument for this command, all channels supported by the current radio mode will be enabled for automatic selection.

Default Either all supported channels are enabled, or only channels 1, 6, and 11 if supported by the current radiomode (e.g. 802.11 b/g).

Format `channel auto-eligible {all | {1-255}}`

Mode AP Profile Radio Config

no channel auto-eligible

The `no` version of this command removes either one or all of the channels currently available for automatic selection from consideration on the radio. If you specify one channel, the command will succeed only if this channel is currently available for automatic selection on the radio. If you supply **all** as the argument for this command, all channels currently available on the radio will be disabled.

Format `no channel auto-eligible {all | {1-255}}`

Mode AP Profile Radio Config

power auto

This command enables auto power adjustment for the radio. This indicates the AP power assignment can be automatically adjusted by the switch.

Default Disabled

Format `power auto`

Mode AP Profile Radio Config

no power auto

The `no` version of this command disables auto power adjustment for the radio.

Format `no power auto`

Mode AP Profile Radio Config

power default

This command configures a power setting for the radio. When auto power adjustment is enabled, this indicates an initial default power setting; otherwise this indicates a fixed power setting.

Default 100%

Format `power default {0-100}`

Mode AP Profile Radio Config

Parameter	*Description*
0–100	Default transmit power percentage.

no power default

The `no` version of this command configures the default power setting to its default value.

Format `no power default`

Mode AP Profile Radio Config

rate

This command is used to configure the list of supported and basic client data rates for the radio. The supported rates are those the AP will allow when setting up communications with client stations. The basic rates are the list of data rates that all stations associating with the AP must support.

Default
- 802.11a supported: 6, 9, 12, 18, 24, 36, 48, 54 Mbps
- 802.11a basic: 6, 12, 24 Mbps
- 802.11b/g supported: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps
- 802.11b/g basic: 1, 2, 5.5, 11 Mbps

Format `rate {basic | supported} value`

Mode AP Profile Radio Config

Parameter	*Description*
value	A valid data rate in Mbps based on radio mode.

no rate

The `no` version of this command is used to remove a basic or supported data rate from the corresponding list.

Format `no rate {basic | supported} value`

Mode AP Profile Radio Config

Parameter	*Description*
value	A valid rate based on radio mode.

rrm

This command enables Radio Resource Measurement (RRM) for the radio. RRM, as defined by the IEEE 802.11k specification, allows for wireless clients to request channel load changes and network neighbor information, as well as to report such information to the AP (and therefore the switch).

Default Enabled

Format `rrm enable`

Mode AP Profile Radio Config

no rrm

The no version of this command disables RRM mode for the radio.

Format `no rrm enable`

Mode AP Profile Radio Config

wmm

This command enables WMM mode for the radio. WMM mode is Wi-Fi Multimedia mode. When enabled QoS settings affect both downstream traffic to the station (AP EDCA parameters) and upstream traffic to the AP (station EDCA parameters). When disabled, QoS only applies to downstream traffic.

Default Enabled

Format `wmm`

Mode AP Profile Radio Config

no wmm

The `no` version of this command disables WMM mode for the radio.

Format `no wmm`

Mode AP Profile Radio Config

load-balance

This command enables load balancing. The optional utilization parameter indicates the percentage of network utilization allowed on the radio before clients are denied. *0%* indicates that no load balancing is performed.

Default
- Disabled
- utilization, 60%

Format `load-balance [utilization {1-100}]`

Mode AP Profile Radio Config

Parameter	*Description*
1–100	Percentage of network utilization allowed on the radio.

no load-balance

The no version of this command disables load balancing or resets the utilization to its default value. If no parameters are entered, load balancing is disabled.

Format `no load-balance [utilization]`

Mode AP Profile Radio Config

dot11n channel-bandwidth

This command selects the bandwidth used in the channel when operating in 802.11n mode.

Default 40 MHz

Format `dot11n channel-bandwidth {20 | 40}`

Mode AP Profile Radio Config

Parameter	*Description*
20	The Radio operates in 20 MHz bandwidth.
40	The Radio operates in 40 MHz bandwidth.

no dot11n channel-bandwidth

The no version of this command sets the bandwidth used to default in the channel when operating in 802.11n mode.

Format `no dot11n channel-bandwidth`

Mode AP Profile Radio Config

dot11n primary-channel

This command selects the bandwidth used in the channel when operating in 802.11n mode.

Default lower

Format `dot11n primary-channel {lower | upper}`

Mode AP Profile Radio Config

Parameter	*Description*
lower	The relative location of the primary channel is on the lower side in the 40 MHz channel.
upper	The relative location of the primary channel is on the upper side in the 40 MHz channel.

no dot11n primary-channel

The `no` version of this command sets the bandwidth used to the default in the channel when operating in 802.11n mode.

Format `no dot11n primary-channel`

Mode AP Profile Radio Config

protection

This command selects the protection mode to use when operating in 802.11n mode. When the protection mode is enabled, AP and stations ensure transmission is protected if there are legacy stations using the same radio frequency.

Default auto

Format `protection {auto | off}`

Mode AP Profile Radio Config

Parameter	*Description*
auto	The protection mechanism is set to *automatic* mode.
off	The protection mechanism is set to *off* mode.

no protection

The `no` version of this command sets the protection mechanism to the default value – automatic mode.

Format `no protection`

Mode AP Profile Radio Config

dot11n short-guard-interval

This command enables or disables the short guard interval when operating in 802.11n mode.

Default enable

Format `dot11n short-guard-interval {enable | disable}`

Mode AP Profile Radio Config

Parameter	*Description*
enable	The short guard interval is enabled. Guard interval is set to 400ns.
disable	The short guard interval is disabled. Guard interval is set to 800ns.

no dot11n short-guard-interval

The `no` version of this command sets the short guard interval to the default.

Format `no dot11n short-guard-interval`

Mode AP Profile Radio Config

dot11n stbc-mode

This command enables or disables the Space Time Block Code (STBC) Mode. The STBC enables the AP to send the same data stream on multiple antennas at the same time.

Default enable

Format `dot11n stbc-mode {enable | disable}`

Mode AP Profile Radio Config

Parameter	*Description*
enable	Send the same data stream on multiple antennas at the same time.
disable	Divide the same data stream between two antennas.

no dot11n stbc-mode

The `no` version of this command sets the stbc-mode to its default value.

Format `no dot11n stbc-mode`

Mode AP Profile Radio Config

multicast tx-rate

This command selects the rate at which the radio transmits the multicast frames.

Default auto

Format `multicast tx-rate rate`

Mode AP Profile Radio Config

Parameter	*Description*
rate	A valid rate based on the radio mode. When the radio is operating in the 5 GHz band, values are 6, 11, 12, 18, 24, 36, 48, and 54 Mbps. When the radio is operating in the 2.4 GHz band, the values are 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54 Mbps. When set to 0, the multicast transmission rate selection is automatic.

no multicast tx-rate

The `no` version of this command sets the multicast transmit rate to 0.

Format `no multicast tx-rate`

Mode AP Profile Radio Config

apsd

This command enables the automatic power save delivery mode for the radio.

Default Enabled

Format `apsd`

Mode AP Profile Radio Config

no apsd

The `no` version of this command disables the automatic power save delivery mode for the radio.

Format `no apsd`

Mode AP Profile Radio Config

incorrect-frame-no-ack

This command configures the radio to not send any acknowledgement for incorrectly received frames.

Default Enabled

Format `incorrect-frame-no-ack`

Mode AP Profile Radio Config

no incorrect-frame-no-ack

The `no` version of this command configures the radio to send the acknowledgement for the incorrectly received frames.

Format `no incorrect-frame-no-ack`

Mode AP Profile Radio Config

show wireless ap profile radio

This command displays the radio configuration for an AP profile. When you enter the required profile ID, a summary view of the radio configuration is displayed. If you enter a radio index, the radio configuration detail is displayed.

Format `show wireless ap profile {1-16} [radio {1-2} [[rates [{advertised | supported}]] | channels]]`

Mode Privileged EXEC

Parameter	*Description*
AP Profile ID	AP profile ID.
Profile Name	Descriptive name associated with the AP Profile ID.
Radio Index	AP profile radio interface.
Status	Indicates whether or not the radio is operational (on or off).
Mode	Indicates the physical layer technology for the radio.
RF Scan - Other Channels Mode	Indicates if the radio is configured to scan on channels other than its operating channel. A radio will always scan on its operating channel.
RF Scan - Other Channels Scan Interval	If the radio is configured to scan other channels, indicates how often, in seconds, the radio will leave its operating channel.
RF Scan - Sentry Mode	Indicates if the radio is configured for dedicated sentry scan mode. In this mode the radio does not allow any client associations.
RF Scan – Sentry Scan Channels	Indicates which set of channels are scanned when sentry scan mode is enabled, for example, **802.11a** indicates the radio will scan all channels within the 802.11a frequency band (5 GHz).

Parameter	*Description*
RF Scan - Scan Duration	Indicates how long the radio will scan on one channel. This configuration applies to both scan other channels mode and sentry scan mode.
Super AG	Indicates if Super AG is enabled on the radio. This can provide better performance by increasing throughput for the radio mode.
Extended Range	Indicates if Extended Range (XR) is enabled on the radio. This is a proprietary method for implementing low rate traffic over long distances.
Enable Broadcast/ Multicast Rate Limiting	Indicates if broadcast and multicast traffic rate limiting is enabled on the radio.
Broadcast/ Multicast Rate Limit	If rate limiting is enabled, broadcast/multicast traffic below this limit is transmitted normally.
Broadcast/ Multicast Rate Limit Burst	If rate limiting is enabled, broadcast/multicast traffic can occur in bursts up to this value before all traffic is considered to exceed the limit.
Beacon Interval	Interval at which the AP transmits beacon frames.
DTIM Period	Indicates the number of beacons between DTIMs (Delivery Traffic Indication Map – indicates buffered broadcast or multicast traffic on the AP).
Fragmentation Threshold	Indicates the size limit for packets transmitted over the network. Packets under configured size are not fragmented.
RTS Threshold (bytes)	Indicates the number of octets in an MPDU, below which an RTS/CTS handshake shall not be performed.
Short Retry Limit	Indicates the maximum number of transmission attempts on frame sizes less than or equal to the RTS Threshold. This is a read-only value and cannot be configured.
Long Retry Limit	Indicates the maximum number of transmission attempts on frame sizes greater than the RTS Threshold. This is a read-only value and cannot be configured.
Maximum Transmit Lifetime	Indicates the elapsed time after the initial transmission of an MSDU, after which further attempts to transmit the MSDU shall be terminated. This is a read-only value and and cannot be configured.
Maximum Receive Lifetime	Indicates the elapsed time after the initial reception of a fragmented MMPDU or MSDU, after which further attempts to reassemble the MMPDU or MSDU shall be terminated. This is a read-only value and cannot be configured.
Maximum Clients	Maximum number of simultaneous associations allowed on the interface.
Automatic Channel Adjustment	Indicates if automatic channel adjustment is enabled. If enabled, the initial AP channel assignment can be automatically adjusted by the switch due to changes in the network.
Automatic Power Adjustment	Indicates if automatic power adjustment is enabled. If enabled, the switch may modify the power on the radio due to changes in performance.
Default Power (%)	Indicates a default power setting for the radio. If automatic power adjustment is disabled, this indicates a fixed power setting, otherwise it indicates the initial power setting before any automatic adjustments.
Load Balancing	Indicates if the AP will load balance users on this radio.
Load Utilization (%)	If load balancing is enabled, % of network utilization allowed on the radio before clients are denied.

Parameter	*Description*
Channel Bandwidth	Indicates the bandwidth used in the channel when the radio is operating in 802.11n mode.
Primary Channel	Specifies the relative location of the primary channel in the 40MHz channel when the radio is operating in 802.11n mode.
802.11n Protection	Indicates if the 802.11n protection mechanism is turned on or off, or if it is in the Auto mode.
Short Guard Interval	Indicates the short guard interval configured on the radio when it is operating in 802.11n mode.
STBC Mode	Indicates the short Space Time Block Code (STBC) mode configured on the radio when it is operating in 802.11n mode.
Multicast Transmit Rate	Indicates the 802.11 rate at which the radio transmits multicast frames.
Automatic Power Save Delivery Mode	Indicates if power save delivery mode is enabled or disabled on the radio.
No Ack	Indicates if acknowledgement has to be sent for incorrectly received frames.
Station Isolation	Indicates whether or not Station Isolation is enabled on the radio. When enabled the AP does not allow data traffic among wireless clients.
Radio Resource Measurement	Indicates if Radio Resource Measurement (RRM) should be enabled for this radio, if supported.

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

```
(Switch) # show wireless ap profile 1 radio 1

AP Profile ID................................. 1
Profile Name.................................. Default
Radio Index................................... 1
Status........................................ On
Mode.......................................... IEEE 802.11g
RF Scan - Other Channels Mode................. Disable
RF Scan - Other Channels Scan Interval........ 60
RF Scan - Sentry Mode......................... Disable
RF Scan - Sentry Scan Channels................ All
RF Scan - Scan Duration....................... 22
Super AG...................................... Disable
Extended Range................................ Disable
Enable Broadcast/Multicast Rate Limiting...... Enable
Broadcast/Multicast Rate Limit................ 50
Broadcast/Multicast Rate Limit Burst.......... 75
Beacon Interval............................... 100
DTIM Period................................... 10
Fragmentation Threshold....................... 2346
RTS Threshold (bytes)......................... 2347
Short Retry Limit............................. 7
Long Retry Limit.............................. 4
Maximum Transmit Lifetime..................... 512
--More-- or (q)uit
Maximum Receive Lifetime...................... 512
Maximum Clients............................... 256
Automatic Channel Adjustment.................. Disable
```

```
Automatic Power Adjustment..................... Disable
Default Power (%).............................. 100
Load Balancing................................. Disable
Load Utilization (%)........................... 60
Channel Bandwidth.............................. 20 MHz
Primary Channel................................ Upper
802.11n Protection............................. Auto
Short Guard Interval........................... Enabled
STBC Mode...................................... Enabled
Multicast Transmit Rate........................ Auto
Automatic Power Save Delivery Mode............. Enabled
No Ack......................................... Enabled
Station Isolation.............................. Disable
Radio Resource Measurement..................... Enable

(Switch) #show wireless ap profile 1 radio 2 channels

AP Profile ID.................................. 1
Profile Name................................... Default
Radio.......................................... 2 - 802.11b/g
Mode........................................... 802.11b/g

Supported Channels (* = Auto-Eligible)
-----------------------------------------------

    1*    2     3     4     5     6*    7     8

    9    10    11*
```

show wireless rates

This command displays the rates valid for a specified physical mode. This is intended to help you determine valid values for the `radio configuration` command.

Format `show wireless rates {a | bg}`

Mode Privileged EXEC

Field	*Description*
Mode	Indicates the physical layer technology to use on the radio.
Valid Rates	Indicates data rates valid for the physical mode.

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

```
(Switch) #show wireless rates a

Mode........................................... IEEE 802.11a

Valid Rates
-----------
6 Mbps
9 Mbps
```

```
12 Mbps
18 Mbps
24 Mbps
36 Mbps
48 Mbps
54 Mbps
```

show wireless multicast tx-rates

This command displays the multicast transmit rates valid for a specified physical mode. This is intended to help you determine valid values for the radio configuration command.

Format `show wireless multicast tx-rates {a | bg}`

Mode Privileged EXEC

Field	*Description*
Mode	Indicates the physical layer technology to use on the radio.
Valid Rates	Indicates data rates valid for the physical mode.

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

```
(Switch) #show wireless rates a

Mode..................................... IEEE 802.11a

Valid Rates
-----------
6 Mbps
9 Mbps
12 Mbps
18 Mbps
24 Mbps
36 Mbps
48 Mbps
54 Mbps
```

Access Point Profile QoS Commands

The commands in this section provide QoS configuration per radio interface and QoS queue within an access point profile.

qos ap-edca

This command configures the downstream traffic flowing from the access point to the client station EDCA queues – voice (0), video (1), best-effort (2), and background (3) queues. The command allows you to configure AIFS (Arbitration Inter-Frame Spacing), Minimum Contention Window, Maximum Contention Window, and Maximum Burst Duration for each of these queues.

Default

- ***Voice***
  AIFS, 1 msec
  Minimum Contention Window, 3 msecs
  Maximum Contention Window, 7 msecs
  Maximum Burst Duration, 1500 usec
- ***Video***
  AIFS, 1 msec
  Minimum Contention Window, 7 msecs
  Maximum Contention Window, 15 msecs
  Maximum Burst Duration, 3000 usec
- ***Best-Effort***
  AIFS, 3 msec
  Minimum Contention Window, 15 msecs
  Maximum Contention Window, 63 msecs
  Maximum Burst Duration, 0 usec
- ***Background***
  AIFS, 7 msec
  Minimum Contention Window, 15 msecs
  Maximum Contention Window, 1023 msecs
  Maximum Burst Duration, 0 usec

Format `qos ap-edca {background | best-effort | video | voice} {aifs {1-255} | cwmin cwmin-time | cwmax cwmax-time | max-burst {0-999900}}`

Mode AP Profile Radio Config

Parameter	*Description*
1–255	Arbitration Inter-Frame Spacing duration value in milliseconds.
cwmin-time	Minimum contention window value in milliseconds.
cwmax-time	Maximum contention window value in milliseconds.
0–999900	Maximum burst length value in microseconds.

no qos ap-edca

The no version of this command resets the chosen queue configuration value for AIFS, Minimum Contention Window, Maximum Contention Window, and Maximum Burst Length to its default value.

Format `no qos ap-edca {background | best-effort | video | voice} {aifs | cwmin | cwmax | max-burst}`

Mode AP Profile Radio Config

qos station-edca

This command configures the upstream traffic flowing from the client station to the access point EDCA queues for voice (0), video (1), best-effort (2), and background (3) queues. The commands allow you to configure AIFS (Arbitration Inter-Frame Spacing), Minimum Contention Window, Maximum Contention Window, and Transmission Opportunity Limit for each of these queues.

Default

- ***Voice***
  AIFS, 2 msec
  Minimum Contention Window, 3 msecs
  Maximum Contention Window, 7 msecs
  Transmission Opportunity Limit, 47 msecs
- ***Video***
  AIFS, 2 msec
  Minimum Contention Window, 7 msecs
  Maximum Contention Window, 15 msecs
  Transmission Opportunity Limit, 94 msecs
- ***Best-Effort***
  AIFS, 3 msec
  Minimum Contention Window, 15 msecs
  Maximum Contention Window, 1023 msecs
  Transmission Opportunity Limit, 0 msecs
- ***Background***
  AIFS, 7 msec
  Minimum Contention Window, 15 msecs
  Maximum Contention Window, 1023 msecs
  Transmission Opportunity Limit, 0 msecs

Format `qos station-edca {background | best-effort | video | voice} {aifs {1-255} | cwmin cwmin-time | cwmax cwmax-time | txop-limit {0-65535}}`

Mode AP Profile Radio Config

Parameter	*Description*
1–255	Arbitration Inter-Frame Spacing duration value in milliseconds.
cwmin-time	Minimum Contention Window value in milliseconds.
cwmax-time	Maximum Contention Window value in milliseconds.
0–65535	Transmission Opportunity Limit value in milliseconds.

no qos station-edca

The no version of this command allows you to reset the chosen queue configuration values for AIFS, Minimum Contention Window, Maximum Contention Window, and Transmission Opportunity Limit.

Format `no qos station-edca {background | best-effort | video | voice} { aifs | cwmin | cwmax | txop-limit}`

Mode AP Profile Radio Config

show wireless ap profile qos

This command displays the configured values for a radio interface per QoS Queue. The various QoS queues that can be displayed are as follows:

- Background (Queue 3), lowest priority queue, high throughput.
- Best Effort (Queue 2), medium priority queue, medium throughput and delay.
- Video (Queue 1), highest priority queue, minimum delay.
- Voice (Queue 0), highest priority queue, minimum delay.

Format `show wireless ap profile {1-16} radio {1-2} qos [{ap-edca | station-edca}]`

Mode Privileged EXEC

Parameter	*Description*
AP Profile ID	Configured AP profile ID.
Profile Name	Name associated with the AP Profile ID.
Radio Index	AP profile radio interface.
Mode	The configured physical mode for the radio.
WMM Mode	Indicates the Wireless Multimedia mode of the radio.
Arbitration Inter-frame Spacing	AP EDCA and station EDCA wait time for data frames, ranges 1–255 milliseconds.
Minimum Contention Window	AP EDCA and station EDCA upper limit of a range from which the initial random back off wait time is determined.
Maximum Contention Window	AP EDCA and station EDCA upper limit for the doubling of the random back off value; doubling continues until either the data frame is sent or this value is reached.
Maximum Burst Length	AP EDCA maximum burst length in microseconds allowed for packet bursts on the wireless network.
Transmission Opportunity Limit	Station EDCA interval of time in milliseconds when a WME client station has the right to initiate transmissions onto the wireless medium.

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

```
Switch# show wireless ap profile 1 radio 1 qos ap-edca
AP Profile ID.............................. 1
Profile Name............................... profile1
Radio Index................................ 1
Mode....................................... IEEE 802.11g
WMM Mode................................... Disable
```

```
QoS             AIFS   Minimum            Maximum            Maximum
Queues                 Contention Window  Contention Window  Burst
--------------  -----  -----------------  -----------------  --------
Voice (0)       1      3                  7                  1500
Video (1)       1      7                  15                 3000
Best-Effort (2) 3      15                 63                 0
Background (3)  7      15                 1023               0

Switch# show wireless ap profile 1 radio 1 qos station-edca
AP Profile ID.................................. 1
Profile Name................................... profile1
Radio Index.................................... 1
Mode........................................... IEEE 802.11g
WMM Mode....................................... Disable

QoS             AIFS   Minimum            Maximum            Tx Op
Queues                 Contention Window  Contention Window  Limit
--------------  -----  -----------------  -----------------  --------
Voice (0)       2      3                  7                  47
Video (1)       2      7                  15                 94
Best-Effort (2) 3      15                 63                 0
Background (3)  7      15                 1023               0
```

Access Point Profile TSPEC Commands

The commands in this section provide Traffic Specification (TSPEC) configuration per radio interface. TSPEC was introduced by the IEEE 802.11e standard that incorporates QoS support in a wireless LAN and is used to provide deterministic service characteristics of time- and delay-sensitive network traffic, such as video and voice, at least to the degree possible in an inherently noisy and unrestricted communications environment.

tspec acm limit

This command defines the maximum amount of wireless network utilization (percentage) to admit for the voice and video access categories, along with an amount of overhead to reserve within each for roaming clients. TSPEC requests in excess of the limit are rejected. Setting the voice or video admission control mandatory (ACM) limit to 0 causes all TSPEC requests to be rejected by the AP for that access category. The sum of the voice and video ACM limits cannot exceed 70 percent.

Note: This command establishes an upper limit for wireless bandwidth to be admitted for the specified access category, but does not guarantee that this limit can actually be reached by the wireless network.

Default `roam-reserve 5, video 15, voice 20`

Format `tspec acm limit {roam-reserve | video | voice} {0-70}`

Mode AP Profile Radio Config

Parameter	*Description*
0–70	Maximum percentage of wireless network utilization to admit for TSPEC requests.

no tspec acm limit

The `no` version of this command sets the specified ACM limit to its corresponding default value.

Format `no tspec acm limit {roam-reserve | video | voice}`

Mode AP Profile Radio Config

tspec acm mode

This command regulates mandatory admission control for the voice and video access categories. When enabled, Wi-Fi Multimedia (WMM) compliant wireless clients must establish a TSPEC with the AP in order to use the specified access category.

Note: Enabling the tspec legacy-wmm-queue-map mode allows legacy (non-WMM compliant) wireless clients to also use the specified access category without establishing a TSPEC.

Default `disabled`

Format `tspec acm mode {video | voice}`

Mode AP Profile Radio Config

no tspec acm mode

The `no` version of this command disables ACM mode for the specified access category.

Format `no tspec acm mode {video | voice}`

Mode AP Profile Radio Config

tspec enable

This command enables overall TSPEC operation for the radio. This is in addition to the ACM mode configuration for each access category.

Default `disabled`

Format `tspec enable`

Mode AP Profile Radio Config

no tspec enable

The `no` version of this command disables overall TSPEC operation for the radio.

Format `no tspec enable`

Mode AP Profile Radio Config

tspec inactivity-timeout

This command specifies the amount of time (in seconds) that an active traffic stream (TS) in the downlink (AP) or uplink (station) may be idle, from the perspective of the AP, before it is deleted by the AP. A value of 0 disables the timeout for the specified direction.

For a bidirectional TS, both the AP and station timeouts must expire in order for the AP to delete the TS due to inactivity. If either of these timeouts are disabled, the AP will not delete a bidirectional TS due to inactivity.

Default `ap 30, station 30`

Format `tspec inactivity-timeout {ap | station} {0-120}`

Mode AP Profile Radio Config

Parameter	*Description*
0–120	Traffic stream inactivity timeout value (in seconds).

no tspec inactivity-timeout

The `no` version of this command sets the specified inactivity timeout to its corresponding default value.

Format `no tspec inactivity-timeout {ap | station}`

Mode AP Profile Radio Config

tspec legacy-wmm-queue-map

This command enables the legacy Wi-Fi Multimedia (WMM) queue map mode. When enabled, the AP allows intermixing of legacy traffic with WMM on access category queues that are operating according to admission control mandatory (ACM) rules. WMM-compliant clients must still establish a valid TSPEC in accordance with ACM operation.

Note: This mode is intended for use with non-WMM enabled (non-WME) clients that share the same wireless network as WME clients. Since non-WME clients do not establish a TSPEC with the AP, the TSPEC admission control may underestimate the available medium time when considering TSPEC requests from WME clients. Use caution when enabling this mode and also consider using very small ACM limit values as well.

Default `Disabled`

Format `tspec legacy-wmm-queue-map`

Mode AP Profile Radio Config

no tspec legacy-wmm-queue-map

The `no` version of this command disables the legacy WMM queue map mode.

Format `no tspec legacy-wmm-queue-map`

Mode AP Profile Radio Config

show wireless ap profile tspec

This command displays the configured TSPEC values for a radio interface.

Format `show wireless ap profile {1-16} radio {1-2} tspec`

Mode Privileged EXEC

Parameter	*Description*
AP Profile ID	Configured AP profile ID.
Profile Name	Name associated with the AP Profile ID.
Radio Index	AP profile radio interface.
Mode	The configured physical mode for the radio.
TSPEC Mode	The overall TSPEC operational mode of the radio.
Voice ACM Mode	The admission control mandatory mode for the voice access category of the radio.
Video ACM Mode	The admission control mandatory mode for the video access category of the radio.
Voice ACM Limit	The admission Control Mandatory bandwidth limit for the voice access category of the radio.
Video ACM Limit	The Admission Control Mandatory bandwidth limit for the video access category of the radio.
Roam Reserve Limit	The ACM bandwidth limit reserved for roaming clients for both the voice and video access categories of the radio.
AP Inactivity Timeout	Inactivity timeout value for traffic streams flowing from the AP to the client station.
STA Inactivity Timeout	Inactivity timeout value for traffic streams flowing from the client station (STA) to the AP.
Legacy WMM Queue Map Mode	A special compatibility mode that allows legacy non Wi-Fi Multimedia clients to gain access to admission controlled access category queue resources, even though they do not use an authorized TSPEC.

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

```
Switch# show wireless ap profile 1 radio 1 tspec
AP Profile ID.............................. 1
Profile Name............................... profile1
Radio...................................... 1 - 802.11b/g/n
Mode....................................... 802.11b/g/n
TSPEC Mode................................. Disabled
Voice ACM Mode............................. Disabled
Video ACM Mode............................. Disabled
Voice ACM Limit (%)........................ 20
Video ACM Limit (%)........................ 15
Roam Reserve Limit (%)..................... 5
AP Inactivity Timeout...................... 30
STA Inactivity Timeout..................... 30
Legacy WMM Queue Map Mode.................. Disabled
```

Access Point Profile VAP Commands

The commands in this section provide Virtual Access Point (VAP) configuration per radio interface within an access point profile.

vap

This command enters the AP Profile VAP configuration mode. In this mode you can modify the VAP configuration parameters of the selected AP profile.

Format `vap {0-15}`

Mode AP Profile Radio Config

Parameter	*Description*
0–15	VAP ID

enable (AP Profile VAP Config Mode)

This command enables the configured VAP on the radio. VAP0 cannot be disabled; if you want to disable VAP0, you must turn off the radio.

Default VAP 0 - Enable, VAP 1–15 - Disable

Format `enable`

Mode AP Profile VAP Config

no enable

The `no` version of this command disables the configured VAP on the radio. This command is not valid for VAP 0.

Format `no enable`

Mode AP Profile VAP Config

network (AP Profile VAP Config Mode)

This command configures the network to apply to the VAP. A VAP must be configured with a network; therefore the network cannot be deleted.

Default The default networks 1–16 are applied to VAP0 – VAP15 in order.

Format `network {1-64}`

Mode AP Profile VAP Config

Parameter	*Description*
1–64	A configured network ID.

WS Managed Access Point Commands

The commands in this section provide views and management of all status and statistics for an access point managed by the Wireless Switch. This includes views of neighbors within the RF area for each managed AP radio interface. This section also lists commands available via Privileged EXEC mode to control the WS Managed APs.

wireless ap channel set

This command sets a new channel on the managed AP radio. The channel is not saved in the configuration, it is maintained until the next time the AP is discovered (AP or switch reset).

Format `wireless ap channel set macaddr radio {1-2} channel`

Mode Privileged EXEC

Parameter	*Description*
macaddr	Managed AP MAC Address.
1–2	Radio interface on the managed AP.
channel	Channel to set on the managed AP.

wireless ap debug

This command sets the admin user password and enables debug mode on the AP (this allows you telnet access to the AP, which is normally disabled in managed mode). The debug mode and required password are not saved in the configuration on the switch, they are only maintained until the next time the AP is discovered (AP or switch reset). This command prompts for the debug password each time it is invoked.

Note: The AP admin user password will remain changed on the AP.

Default Disable

Format `wireless ap debug macaddr`

Mode Privileged EXEC

Parameter	*Description*
macaddr	Managed AP MAC Address.

no wireless ap debug

The no version of this command disables AP debug mode. The managed AP UI will be disabled as it normally is when the AP is in managed mode.

Format `no wireless ap debug macaddr`

Mode Privileged EXEC

wireless ap download image-type

This command sets a TFTP path and file name for the specified AP system type. The download request can be initiated for all the image types or for a specific image type.

Default None

Format `wireless ap download image-type {1-2} {url}`

Mode Privileged EXEC

Parameter	*Description*
1–2	The image type.
url	TFTP file path for an AP system image.

Example: The following shows an example of the command.

```
(Switching) #wireless ap download image-type 1 tftp://1.1.1.1/./ap/apcode.tar ?
<cr>    Press Enter to execute the command.
```

wireless ap download group-size

This command sets the download group size. The switch requests the managed APs to download a new system image in groups. By default the switch will request the download for 10 managed APs at a time.

Default 10

Format `wireless ap download group-size {1-48}`

Mode Privileged EXEC

Parameter	*Description*
1–48	Enter the number of APs.

Example: The following shows an example of the command.

```
(Switching) #wireless ap download group-size 3
```

wireless ap download abort

This command aborts the AP image download process. If the process is aborted, the code download still continues on the remaining APs in the current download group, but not on APs in the next download group.

Format `wireless ap download abort`

Mode Privileged EXEC

wireless ap download start

This command initiates the AP image download process to (a) all managed APs running a specific image type, or to (b) one or all managed APs irrespective of image type, to download a new system image based on the configured TFTP URL. The download is not started if the filename for the requested image type is not configured.

Format `wireless ap download start [image-type {1-2}] [macaddr]`

Mode Privileged EXEC

Parameter	*Description*
1–2	The image type.
macaddr	Managed AP MAC Address.

Example: The following shows an example of the command.

```
(Switching) #wireless ap download start image-type 1

(Switching) #wireless ap download start

(Switching) #wireless ap download start 00:00:84:00:50
```

wireless ap power set

This command sets a new power on the managed AP radio. The power setting is not saved in the configuration, it is maintained until the next time the AP is discovered (AP or switch reset).

Format `wireless ap power set macaddr radio {1-2} {1-100}`

Mode Privileged EXEC

Parameter	*Description*
macaddr	Managed AP MAC Address.
1–2	Radio Index to be configured on the managed AP.
1–100	Power to be configured for the radio on the managed AP.

wireless ap reset

This command requests the switch to reset the managed AP indicated by the MAC address.

Format `wireless ap reset macaddr`

Mode Privileged EXEC

Parameter	*Description*
macaddr	Managed AP MAC address.

clear wireless ap failed

This command deletes one or all managed AP entries with a failed status. A failed status indicates the Wireless Switch has lost contact with the managed AP.

Format `clear wireless ap failed [macaddr]`

Mode Privileged EXEC

Parameter	*Description*
macaddr	Managed AP MAC Address.

Example: The following shows an example of the command.

```
(Switch) #clear wireless ap failed
Are you sure you want to clear all failed managed AP entries? (y/n) y
All managed AP failed entries cleared.
```

clear wireless ap rrm neighbors

This command deletes all neighbor information pertaining to Radio Resource Measurement (RRM) for all managed APs.

Format `clear wireless ap rrm neighbors`

Mode Privileged EXEC

Example: The following shows an example of the command.

```
(DWS-4026) #clear wireless rrm neighbors
```

clear wireless ap neighbors

This command deletes entries from the managed AP client and AP neighbor lists. Note that client neighbor entries added via a client association to the managed AP will not be cleared; these are only removed by the system when a client disassociates.

Format `clear wireless ap neighbors macaddr`

Mode Privileged EXEC

Example: The following shows an example of the command.

```
(DWS-4026) #clear wireless ap neighbors
Are you sure you want to clear managed AP neighbors (associated client neighbors will not be
cleared)? (y/n) y
Managed AP neighbor entries cleared.
```

show wireless ap status

This command displays operational status for a WS managed AP. If no parameters are specified, a summary of all managed APs is displayed. If an AP MAC address is specified, the detailed status is displayed.

If the Wireless Switch is a Cluster Controller, the command show all the APs managed by the peer group.

When acting as a Cluster Controller, the peer managed APs are displayed with an “*” (asterisk symbol) before the AP MAC Address in the summary command.

Format `show wireless ap [macaddr] status`

Mode Privileged EXEC

Field	*Description*
macaddr	WS managed AP MAC address.
MAC Address	The Ethernet address of the WS managed AP.
Location	A location description for the AP, this is the value configured in the valid AP database (either locally or on the RADIUS server).

Field	*Description*
IP Address	The network IP address of the managed AP.
IP Subnet Mask	The network mask of the managed AP.
Managing Switch	Indicates if the AP is managed by this Wireless Switch or a peer Wireless Switch.
Switch MAC Address	The Ethernet address of the Wireless Switch managing the AP.
Switch IP Address	The network IP address of the Wireless Switch managing the AP.
Status	The current managed state of the AP. The possible values are: • Discovered - The AP is discovered by the switch, but is not yet authenticated. • Upgrading - The AP has been validated. The AP code image is upgraded as it does not match the version stored on the wireless switch. This status displays only if the Integrated AP Image Mode is supported by the wireless switch. • Authenticated - The AP has been validated and authenticated (if authentication is enabled), but it is not configured. • Managed - The AP profile configuration has been applied to the AP and it is operating in managed mode. • Failed - The switch lost contact with the AP. A failed entry will remain in the managed AP database unless you remove it. Note that a managed AP will temporarily show a failed status during a reset.
Configuration Status	This status indicates if the AP is configured successfully with the assigned profile.
Last Failing Configuration Element	The element ID of the last failing configuration element. If the configuration status indicates a partial or complete failure, this field indicates the last element that failed during configuration.
Configuration Failure Error	An ASCII string provided by the AP containing an error message for the last failing configuration element.
Debug Mode	Indicates whether or not debug mode is enabled on the AP. Debug mode allows you telnet access to the device.
Code Download Status	Indicates the current status of a code download request for this AP.
Reset Status	Indicates the current status of an AP reset, if one has been initiated.
Profile	The AP profile configuration currently applied to the managed AP, the profile is assigned to the AP in the valid AP database. ***Note:*** Once an AP is discovered and managed by the switch, if the profile is changed in the valid AP database (either locally or on the RADIUS server) the AP must be reset to configure with the new profile.
Vendor ID	Vendor of the AP software, this is learned from the AP during discovery.
Protocol Version	Indicates the protocol version supported by the software on the AP; this is learned from the AP during discovery.
Software Version	Indicates the version of software on the AP; this is learned from the AP during discovery.
Hardware Type	Hardware platform for the AP; this is learned from the AP during discovery.
Serial Number	Unique Serial number assigned to the AP; this is learned from the AP during discovery.
Part Number	Hardware part number for the AP; this is learned from the AP during discovery.

Field	*Description*
Discovery Reason	This status value indicates how the managed AP was discovered. The status is one of the following values: • IP Poll Received - The AP was discovered via an IP poll from the switch; its IP address is configured in the IP polling list. • Peer Redirect - The AP was discovered through a peer switch redirect, the AP tried to associate with another peer switch and learned the current switch IP address from the peer (peer learned switch IP address in RADIUS server response when validating the AP.) • Switch IP Configured - The managed AP is configured with the switch IP address. • Switch IP DHCP - The managed AP learned the correct switch IP address through DHCP option 43. • L2 Poll Received - The AP was discovered through the Broadcom Wireless Device Discovery Protocol.
Authenticated Clients	Total number of clients currently authenticated to the AP. This is the sum of all authenticated clients for all the VAPs enabled on the AP.
System Uptime	Time in seconds since last power-on reset of the managed AP.
Age	Time since last communication between the WDS and the AP.

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

On the Cluster Controller the summary command displays entries in the following format:

```
(DWS-4026) #show wireless ap status

    MAC Address                                    Configuration
 (*) Peer Managed    IP Address    Profile Status     Status           Age
------------------ -------------- ------- ------- ------------ --------------
*00:00:85:00:50:00 192.168.37.49   1       Managed Success       0d:00:00:11

On the switch that is not acting as a Cluster Controller the summary command displays entries in
the following format:
(DWS-4026) #show wireless ap status

                                                 Configuration
   MAC Address      IP Address    Profile Status     Status           Age
------------------ -------------- ------- ------- ------------ --------------
00:00:85:00:50:00 192.168.37.49   1       Managed Success       0d:00:00:01

(DWS-4026) #show wireless ap 00:22:B0:3A:C1:80 status

MAC address..................................... 00:22:B0:3A:C1:80
Location.....................................
IP Address...................................... 10.27.64.126
IP Subnet Mask.................................. 255.255.254.0
Managing Switch................................. Local Switch
Switch MAC Address.............................. 00:02:BC:00:00:77
Switch IP Address............................... 10.27.65.8
Status.......................................... Managed
Configuration Status............................ Success
Last Failing Configuration Element.............. None
Configuration Failure Error...................
Debug Mode...................................... Disable
```

```
Code Download Status..... Not Started
Reset Status..... Not Started
Profile..... 1 - Default
Vendor ID.....
Protocol Version..... 2
Software Version..... D.05.22.1
Hardware Type..... 9 - AP-86 Dual Radio a/b/g/n
Serial Number..... H05167353
Part Number..... dwl8600ap
Discovery Reason..... L2 Poll Received
Authenticated Clients..... 0
System Up Time..... 0d:00:02:43
Age..... 0d:00:00:02#
```

show wireless ap tspec status

This command displays operational TSPEC status for the specified WS managed AP.

Format `show wireless ap [macaddr] tspec status`

Mode Privileged EXEC

Field	*Description*
macaddr	WS managed AP MAC address.
MAC Address	The Ethernet address of the WS managed AP.
Access Category	Identifies the access category to which the following values pertain.
Number of Active Traffic Streams	The current number of traffic streams for the designated access category of the WS managed AP.
Number of Traffic Stream Clients	The current number of wireless clients with at least one traffic stream for the designated access category of the WS managed AP.
Number of Traffic Stream Roaming Clients	The current number of wireless roaming clients with at least one traffic stream for the designated access category of the WS managed AP. This value is included in the Num Traffic Stream Clients listed above.

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

```
(Switch) #show wireless ap 00:01:01:02:01:01 tspec status

MAC Address..... 00:01:01:02:01:01
Location..... FirstFloor

Access Category..... Voice
Number of Active Traffic Streams..... 0
Number of Traffic Stream Clients..... 0
Number of Traffic Stream Roaming Clients..... 0

Access Category..... Video
Number of Active Traffic Streams..... 0
Number of Traffic Stream Clients..... 0
Number of Traffic Stream Roaming Clients..... 0
```

show wireless ap radio status

This command displays operational status for a WS managed AP radio interface. If no parameters are specified, a summary of radio status for all managed APs is displayed. If an AP MAC address and radio interface are specified, the detailed status is displayed.

The Cluster Controller displays the peer managed AP with an * (asterisk) before the AP MAC Address in the summary command.

Format `show wireless ap {macaddr radio [{1-2}] status | radio status}`

Mode Privileged EXEC

Field	*Description*
macaddr	WS managed AP MAC address.
1–2	The radio interface on the AP.
MAC Address	The Ethernet address of the WS managed AP.
Location	A location description for the AP, this is the value configured in the valid AP database (either locally or on the RADIUS server).
Radio	Indicates the radio interface on the AP.
Channel	If the radio is operational, the current operating channel for the radio.
Bandwidth	If the radio is operational, the current channel bandwidth in use.
Transmit Power	If the radio is operational, the current transmit power for the radio.
Associated Clients	Total count of clients associated on the physical radio, this is a sum of all the clients associated to each VAP enabled on the radio.
Total Neighbors	Total number of neighbors (both APs and clients) that can be seen by this radio in its RF area.
Supported Channels	The list of eligible channels the AP reported to the switch for channel assignment. This list is based on country code, hardware capabilities, and any configured channel limitations.
Fixed Channel Indicator	This flag indicates if a fixed channel is configured and assigned to the radio. A fixed channel can be configured in the valid AP database (locally or on a RADIUS server).
Manual Channel Adjustment Status	Indicates the current state of a manual request to change the channel on this radio.
Fixed Power Indicator	This flag indicates if a fixed power setting is configured and assigned to the radio. A fixed transmit power can be configured in the valid AP database (locally or on a RADIUS server).
Manual Power Adjustment Status	Indicates the current state of a manual request to change the power setting on this radio.
WLAN Utilization	Indicates the total network utilization for the physical radio. This value is based on radio statistics.

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

On the Cluster Controller, the summary command will display entries in the following format:

On the switch that is not acting as a Cluster Controller the summary command displays entries in the

following format:

```
(Switch) #show wireless ap radio status

    MAC Address                                      Transmit   Assoc.  Auth.
 (*) Peer Managed       Location        Radio Channel Power (%) Clients Clients
------------------ ------------------- ----- ------- --------- ------- -------
*00:00:85:00:50:00 ap-5                1     11      100       0       0
                                       2     153     100       0       0
```

On the switch that is not acting as a Cluster Controller, the summary command displays entries in the following format:

```
(Switch) #show wireless ap radio status

                                                    Transmit   Assoc.  Auth.
   MAC Address         Location        Radio Channel Power (%) Clients Clients
---------------- ------------------- ----- ------- --------- ------- -------
00:00:85:00:50:00 ap-5                1     1       100       0       1
                                      2     153     100       0       0

(Switch) #
(Switch) #show wireless ap 00:01:01:02:01:01 radio 1 status

MAC Address..................................... 00:01:01:02:01:01
Location........................................ FirstFloor
Radio........................................... 1
Eligible Channels............................... 1, 6, 11
Channel......................................... 0
Bandwidth....................................... 20MHz
Fixed Channel Indicator......................... No
Manual Channel Adjustment Status................ Not Started
Transmit Power.................................. 0
Fixed Power Indicator........................... No
Manual Power Adjustment Status.................. Not Started
Associated Clients.............................. 2
Total Neighbors................................. 0
WLAN Utilization................................ 0
(Switch) #
```

show wireless ap radio channel status

This command displays the manual channel adjustment status for a radio on a WS managed AP. This indicates the individual AP status for a wireless channel plan apply request or a wireless AP channel set request.

Format `show wireless ap macaddr radio {1-2} channel status`

Mode Privileged EXEC

Field	*Description*
macaddr	WS managed AP MAC address.
1–2	Radio Interface.
Channel	If the radio is operational, the current operating channel for the radio.
Manual Channel Adjustment Status	Indicates the current state of a manual request to change the channel on this radio.

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

```
(Switch) #show wireless ap 00:01:01:02:01:01 radio 2 channel status

Manual Channel Adjustment Status.............. In Progress
Channel....................................... 6

(Switch) #
```

show wireless ap radio power status

This command displays the manual power adjustment status for a radio on a WS managed AP. This indicates the individual AP status for a wireless power plan apply request or a wireless AP power set request.

Format `show wireless ap macaddr radio {1-2} power status`

Mode Privileged EXEC

Field	*Description*
macaddr	WS managed AP MAC address.
1–2	Radio Interface.
Transmit Power	If the radio is operational, the current transmit power for the radio.
Manual Power Adjustment Status	Indicates the current state of a manual request to change the power setting on this radio.

show wireless ap radio tspec status

This command displays operational TSPEC status for a WS managed AP radio interface.

Format `show wireless ap macaddr radio {1-2} tspec status`

Mode Privileged EXEC

Field	*Description*
macaddr	WS managed AP MAC address.
1–2	The radio interface on the AP.
MAC Address	The Ethernet address of the WS managed AP.
Location	A location description for the AP, this is the value configured in the valid AP database (either locally or on the RADIUS server).
Radio	Indicates the radio interface on the AP.
Access Category	Identifies the access category to which the following values pertain.
Operational Status	The current operational status of the designated access category on this radio.
Number of Active Traffic Streams	The current number of traffic streams for the designated access category on this radio.
Number of Traffic Stream Clients	The current number of wireless clients with at least one traffic stream for the designated access category on this radio.
Number of Traffic Stream Roaming Clients	The current number of wireless roaming clients with at least one traffic stream for the designated access category on this radio. This value is included in the Num Traffic Stream Clients listed above.
Medium Time Admitted	Current sum of all medium times currently allocated to wireless clients with one or more traffic streams for the designated access category on this radio. This value is in units of 32 microseconds-per-second (usecs/sec).
Medium Time Unallocated	Amount of configured medium time available for non-roaming and roaming clients for the designated access category on this radio. This value is in units of 32 microseconds-per-second (usecs/sec).
Medium Time Roaming Unallocated	Amount of configured medium time available for roaming clients only for the designated access category on this radio. This value is in units of 32 microseconds-per-second (usecs/sec).

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

```
(Switch) #show wireless ap 00:01:01:02:01:01 radio 1 tspec status

MAC Address..................................... 00:01:01:02:01:01
Location........................................ FirstFloor
Radio........................................... 1

Access Category................................. Voice
Operational Status.............................. Enabled
Number of Active Traffic Streams................ 0
Number of Traffic Stream Clients................ 0
Number of Traffic Stream Roaming Clients....... 0
```

```
Medium Time Admitted.......................... 0
Medium Time Unallocated....................... 4687
Medium Time Roaming Unallocated............... 6250

Access Category............................... Video
Operational Status............................ Enabled
Number of Active Traffic Streams.............. 0
Number of Traffic Stream Clients.............. 0
Number of Traffic Stream Roaming Clients...... 0
Medium Time Admitted.......................... 0
Medium Time Unallocated....................... 3125
Medium Time Roaming Unallocated............... 4687
```

show wireless ap radio vap status

This command displays the operational status for WS managed AP Virtual AP (VAP) interfaces. If no parameters are specified, a summary of all VAPs for a managed AP is displayed. If a VAP ID is specified, the detailed status is displayed.

Format `show wireless ap macaddr radio {1-2} vap [{0-15}] status`

Mode Privileged EXEC

Field	*Description*
macaddr	WS managed AP MAC address.
1–2	The radio interface on the AP.
0–15	VAP ID.
MAC Address	The Ethernet address of the WS managed AP.
Location	A location description for the AP, this is the value configured in the valid AP database (either locally or on the RADIUS server).
Radio	Indicates a radio interface on the AP.
VAP ID	The integer ID used to identify the VAP *(0–7)*, this is used to uniquely identify the VAP for configuration via CLI/SNMP.
VAP MAC Address	The Ethernet address of the VAP.
SSID	Indicates the network assigned to the VAP. The network for each VAP is configured within the AP profile and the SSID is based on the network configuration.
Client Assoc	Indicates the total number of clients currently associated to the VAP.

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

```
(Switch) #show wireless ap 00:01:01:02:01:01 radio 1 vap status

MAC Address................................... 00:01:01:02:01:01
Location...................................... FirstFloor
Radio......................................... 1

                                                 Client
VAP ID   VAP MAC Address           SSID           Assoc.
```

```
------ ------------------ ----------------------- ------
0      00:01:01:02:01:01   Guest Network           0
1      00:01:01:02:01:02   Managed SSID 2          0
2      00:01:01:02:01:03   Managed SSID 3          0
3      00:01:01:02:01:04   Managed SSID 4          0
4      00:01:01:02:01:05   Managed SSID 5          0
5      00:01:01:02:01:06   Managed SSID 6          0
6      00:01:01:02:01:07   Managed SSID 7          0
7      00:01:01:02:01:08   Managed SSID 8          0

(Switch) #show wireless ap 00:22:B0:3A:C1:80 radio 1 vap 2 status

MAC address.................................. 00:22:B0:3A:C1:80
Location..................................... FirstFloor
Radio........................................ 1 - 802.11a/n
VAP ID....................................... 2
VAP MAC Address.............................. 00:22:B0:3A:C1:80
SSID......................................... Managed SSID 3
Client Authentications....................... 0
```

show wireless ap radio vap tspec status

This command displays operational TSPEC status for WS managed AP Virtual AP (VAP) interfaces.

Format `show wireless ap macaddr radio {1-2} vap [{0-15}] tspec status`

Mode Privileged EXEC

Field	*Description*
macaddr	WS managed AP MAC address.
1–2	The radio interface on the AP.
0–15	VAP ID
MAC Address	The Ethernet address of the WS managed AP.
Location	A location description for the AP, this is the value configured in the valid AP database (either locally or on the RADIUS server).
Radio	Indicates a radio interface on the AP.
VAP ID	The integer ID used to identify the VAP (0–7), this is used to uniquely identify the VAP for configuration via CLI/SNMP.
VAP MAC Address	The Ethernet address of the VAP.
SSID	Indicates the network assigned to the VAP. The network for each VAP is configured within the AP profile and the SSID is based on the network configuration.
Access Category	Identifies the access category to which the following values pertain.
Operational Status	The current operational status of the designated access category on this VAP.
Number of Active Traffic Streams	The current number of traffic streams for the designated access category on this VAP.
Number of Traffic Stream Clients	The current number of wireless clients with at least one traffic stream for the designated access category on this VAP.

Field	*Description*
Number of Traffic Stream Roaming Clients	The current number of wireless roaming clients with at least one traffic stream for the designated access category on this VAP. This value is included in the Num Traffic Stream Clients listed above.
Medium Time Admitted	Current sum of all medium times currently allocated to wireless clients with one or more traffic streams for the designated access category on this VAP. This value is in units of 32 microseconds-per-second (usecs/sec).
Medium Time Unallocated	Amount of configured medium time available for non-roaming and roaming clients for the designated access category on this VAP. This value is in units of 32 microseconds-per-second (usecs/sec).
Medium Time Roaming Unallocated	Amount of configured medium time available for roaming clients only for the designated access category on this VAP. This value is in units of 32 microseconds-per-second (usecs/sec).

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

```
(Switch) #show wireless ap 00:01:01:02:01:01 radio 1 vap 2 tspec status
MAC Address..................................... 00:01:01:02:01:01
Location........................................ FirstFloor
Radio........................................... 1
VAP ID.......................................... 2
VAP MAC Address................................. 00:01:01:02:01:03
SSID............................................ Managed SSID 3

Access Category................................. Voice
Operational Status.............................. Enabled
Number of Active Traffic Streams................ 0
Number of Traffic Stream Clients................ 0
Number of Traffic Stream Roaming Clients....... 0
Medium Time Admitted............................ 0
Medium Time Unallocated......................... 4687
Medium Time Roaming Unallocated................. 6250

Access Category................................. Video
Operational Status.............................. Enabled
Number of Active Traffic Streams................ 0
Number of Traffic Stream Clients................ 0
Number of Traffic Stream Roaming Clients....... 0
Medium Time Admitted............................ 0
Medium Time Unallocated......................... 3125
Medium Time Roaming Unallocated................. 4687
```

show wireless ap radio neighbor ap status

This command displays the status parameters for each neighbor AP detected through an RF scan on the specified managed AP radio.

Format `show wireless ap macaddr radio {1-2} neighbor ap status`

Mode Privileged EXEC

Field	*Description*
macaddr	WS managed AP MAC address.
1–2	The radio interface on the AP.
MAC Address	The Ethernet address of the WS managed AP.
Location	A location description for the AP, this is the value configured in the valid AP database (either locally or on the RADIUS server).
Radio	Indicates a radio interface on the AP.
Neighbor AP MAC	The Ethernet MAC address of the neighbor AP network, this could be a physical radio interface or VAP MAC address. For Broadcom APs, this is always a VAP MAC address. The neighbor AP MAC address may be cross-referenced in the RF Scan status.
SSID	Service Set ID of the neighbor AP network.
RSSI	Received Signal Strength Indication, this is an indicator of the signal strength relative to the neighbor and may give an idea of the neighbor's distance from the managed AP.
Status	Indicates the managed status of the AP, whether this is a valid AP known to the switch or a Rogue on the network. The valid values are: • Managed - The neighbor AP is managed by this switch or another switch within the peer group. The neighbor AP status can be referenced using its base MAC address. • Unknown- The neighbor APs detected in the RF scan are initially categorized as *Unknown* APs. • Standalone - The AP is managed in standalone mode and configured as a valid AP entry (local or RADIUS). • Rogue - The AP intrusion Detection function has determined that the AP is posing a threat to the network and categorizes the neighbor AP as *Rogue*.
Age	Indicates the time since this AP was last reported from an RF scan on the radio.

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

```
(Switch) #show wireless ap 00:01:01:02:01:01 radio 1 neighbor ap status

MAC Address..................................... 00:01:01:02:01:01
Location........................................ FirstFloor
Radio........................................... 1

 Neighbor AP MAC              SSID              RSSI     Status          Age
----------------- --------------------------- ---- --------------- -----------
00:01:01:02:01:03 Network3                     10   Managed         0h:2m:52s
00:01:01:02:03:02 Network2                     10   Managed         0h:2m:55s
00:33:01:02:01:83 Lobby                        10   Unknown         0h:2m:49s
```

show wireless ap radio neighbor client status

This command displays the status parameters for each client detected as a neighbor to the specified managed AP radio. A client neighbor may be detected through one or more methods: RF scan on the radio, client association to a VAP on the radio, or receiving a probe request from the client.

Format `show wireless ap macaddr radio {1-2} neighbor client status`

Mode Privileged EXEC

Field	*Description*
macaddr	WS managed AP MAC address.
1–2	The radio interface on the AP.
MAC Address	The Ethernet address of the WS managed AP.
Location	A location description for the AP, this is the value configured in the valid AP database (either locally or on the RADIUS server).
Radio	Indicates a radio interface on the AP.
Neighbor Client MAC	The Ethernet address of the client station.
RSSI	Received Signal Strength Indication, this is an indicator of the signal strength relative to the neighbor and may give an idea of the neighbor's distance from the managed AP.
Channel	The managed AP channel the client frame was received on, which may be different than the operating channel for this radio.
Discovery Reason	Indicates one or more discovery methods for the neighbor client. One of more of the following abbreviated values may be displayed: • RF Scan (RF) - The client was reported from an RF scan on the radio. Note that client stations are difficult to detect via RF scan; the other methods are more common for client neighbor detection. • Probe Request (Probe) - The managed AP received a probe request from the client. • Associated to Managed AP (Assoc Managed AP) - This neighbor client is associated to another managed AP. • Associated to this AP (Assoc this AP) - The client is associated to this managed AP on the displayed radio. • Associated to Peer AP (Assoc peer AP) - The client is associated to a peer switch managed AP. • Ad Hoc Rogue (Ad Hoc) - The client was detected as part of an Ad Hoc network.
Age	Indicates the time since this client was last reported from an RF scan on the radio.

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

```
(Switch) #show wireless ap 00:01:01:02:01:01 radio 1 neighbor client status

MAC Address..................................... 00:01:01:02:01:01
Location........................................ FirstFloor
Radio........................................... 1

Neighbor MAC      RSSI Channel Discovery Reason           Age
----------------- ---- ------- ------------------------- ----------------
```

```
00:01:01:10:01:01 20   6       Assoc this AP,Probe        00d:00h:05m:21s
00:01:01:14:01:01 20   6       Assoc this AP,Probe        00d:00h:05m:20s
00:01:31:16:01:01 20   11      Probe,RF                   00d:00h:05m:19s
```

show wireless ap statistics

This command displays global statistics for a managed AP, the managed AP MAC address parameter is required, and the command displays a detailed view of the current statistics. You can clear all wireless statistics through the `clear wireless statistics` command.

Format `show wireless ap macaddr statistics`

Mode Privileged EXEC

Field	*Description*
macaddr	Managed AP MAC address.
MAC Address	The Ethernet address of the WS managed AP.
Location	A location description for the AP, this is the value configured in the valid AP database (either locally or on the RADIUS server.)
WLAN Packets Received	The total packets received by the AP on the wireless network.
WLAN Bytes Received	Total bytes received by the AP on the wireless network.
WLAN Packets Transmitted	Total packets transmitted by the AP on the wireless network.
WLAN Bytes Transmitted	Total bytes transmitted by the AP on the wireless network.
WLAN Packets Receive Dropped	Total receive packets discarded by the AP on the wireless network.
WLAN Bytes Received	Total receive bytes discarded by the AP on the wireless network.
WLAN Packets Transmitted	Total packets discarded by the AP prior to transmission on the wireless network.
WLAN Bytes Transmitted	Total bytes discarded by the AP prior to transmission on the wireless network.
Ethernet Packets Received	Total packets received by the AP on the wired network.
Ethernet Bytes Received	Total bytes received by the AP on the wired network.
Ethernet Multicast Packets Received	Total multicast packets received by the AP on the wired network.
Ethernet Packets Transmitted	Total packets transmitted by the AP on the wired network.
Ethernet Bytes Transmitted	Total bytes transmitted by the AP on the wired network.
Total Transmit Errors	Total transmit errors detected by the AP on the wired network.
Total Receive Errors	Total receive errors detected by the AP on the wired network.
ARP Reqs Converted from Bcast to Ucast	Total number of ARP request converted from broadcast to unicast on the wireless network.
Filtered ARP Requests	Total number of ARP requests filtered by the AP instead of sending on the wireless network.
Broadcasted ARP Requests	Total number of ARP requests broadcasted on the wireless network after performing wireless ARP suppression.

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

```
(Switch) #show wireless ap 00:01:01:02:01:01 statistics

MAC Address..................................... 00:01:01:02:01:01
Location........................................ FirstFloor
WLAN Packets Received........................... 0
WLAN Packets Transmitted........................ 0
WLAN Bytes Received............................. 0
WLAN Bytes Transmitted.......................... 0
WLAN Packets Receive Dropped.................... 0
WLAN Packets Transmit Dropped................... 0
WLAN Bytes Receive Dropped...................... 0
WLAN Bytes Transmit Dropped..................... 0
Ethernet Packets Received....................... 0
Ethernet Packets Transmitted.................... 0
Ethernet Bytes Received......................... 0
Ethernet Bytes Transmitted...................... 0
Ethernet Multicast Packets Received............. 0
Total Transmit Errors........................... 0
Total Receive Errors............................ 0
ARP Reqs Converted from Bcast to Ucast......... 50
Filtered ARP Requests........................... 8
Broadcasted ARP Requests........................ 5

(Switch) #
```

show wireless ap tspec statistics

This command displays TSPEC global statistics for a managed AP, the managed AP MAC address parameter is required, and the command displays a detailed view of the current statistics. The administrator can clear all wireless statistics through the clear wireless statistics command.

Format `show wireless ap macaddr tspec statistics`

Mode Privileged EXEC

Field	*Description*
macaddr	WS managed AP MAC address.
MAC Address	The Ethernet address of the WS managed AP.
Location	A location description for the AP, this is the value configured in the valid AP database (either locally or on the RADIUS server).
Access Category	Identifies the access category to which the following values pertain.
Total TSPEC Packets Received	Total packets received by the AP on the wireless network for all traffic streams belonging to the designated access category.
Total TSPEC Packets Transmitted	Total packets transmitted by the AP on the wireless network for all traffic streams belonging to the designated access category.
Total TSPEC Bytes Received	Total bytes received by the AP on the wireless network for all traffic streams belonging to the designated access category.

Field	*Description*
Total TSPEC Bytes Transmitted	Total bytes transmitted by the AP on the wireless network for all traffic streams belonging to the designated access category.
Total TSPECs Accepted	Total number of TSPECs accepted by the AP on the wireless network for the designated access category.
Total TSPECs Rejected	Total number of TSPECs rejected by the AP on the wireless network for the designated access category.
Total Roaming TSPECs Accepted	Total number of TSPECs accepted from roaming clients by the AP on the wireless network for the designated access category. This value is included in the Total TSPECs Accepted value above.
Total Roaming TSPECs Rejected	Total number of TSPECs rejected from roaming clients by the AP on the wireless network for the designated access category. This value is included in the Total TSPECs Rejected value above.

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

```
(Switch) #show wireless ap 00:01:01:02:01:01 statistics

MAC Address..................................... 00:01:01:02:01:01
Location........................................ FirstFloor

Access Category................................. Voice
Total TSPEC Packets Received.................... 0
Total TSPEC Packets Transmitted................. 0
Total TSPEC Bytes Received...................... 0
Total TSPEC Bytes Transmitted................... 0
Total TSPECs Accepted........................... 0
Total TSPECs Rejected........................... 0
Total Roaming TSPECs Accepted................... 0
Total Roaming TSPECs Rejected................... 0

Access Category................................. Video
Total TSPEC Packets Received.................... 0
Total TSPEC Packets Transmitted................. 0
Total TSPEC Bytes Received...................... 0
Total TSPEC Bytes Transmitted................... 0
Total TSPECs Accepted........................... 0
Total TSPECs Rejected........................... 0
Total Roaming TSPECs Accepted................... 0
Total Roaming TSPECs Rejected................... 0
```

show wireless ap radio statistics

This command displays statistics for each physical radio on a WS managed AP, the managed AP MAC address and radio parameters are required, the command displays a detailed view of the current statistics.

Format `show wireless ap macaddr radio {1-2} statistics`

Mode Privileged EXEC

Field	*Description*
macaddr	WS managed AP MAC address.
1–2	The radio interface on the AP.
MAC Address	The Ethernet address of the WS managed AP.
Location	A description for the AP, this is the value configured in the valid AP database (either locally or on the RADIUS server).
Radio	Indicates a radio interface on the AP.
WLAN Packets Received	Total packets received by the AP on this radio interface.
WLAN Bytes Received	Total bytes received by the AP on this radio interface.
WLAN Packets Transmitted	Total packets transmitted by the AP on this radio interface.
WLAN Bytes Transmitted	Total bytes transmitted by the AP on this radio interface.
WLAN Packets Receive Dropped	Total receive packets discarded by the AP on this radio interface.
WLAN Bytes Received	Total receive bytes discarded by the AP on this radio interface.
WLAN Packets Transmitted	Total packets discarded by the AP prior to transmission on this radio interface.
WLAN Bytes Transmitted	Total bytes discarded by the AP prior to transmission on this radio interface.
Transmitted Fragment Count	Count of acknowledged MPDU with an individual address or an MPDU with a multicast address of type Data or Management.
Multicast Transmitted Frame Count	Count of successfully transmitted MSDU frames where the multicast bit is set in the destination MAC address.
Failed Count	Number of times an MSDU is not transmitted successfully due to transmit attempts exceeding either the short retry limit or the long retry limit.
Retry Count	Number of time an MSDU is successfully transmitted after one or more retries.
Multiple Retry Count	Number of times an MSDU is successfully transmitted after more than one retry.
Frame Duplicate Count	Number of times a frame is received and the Sequence Control field indicates it is a duplicate.
RTS Success Count	Count of CTS frames received in response to an RTS frame.
RTS Failure Count	Count of CTS frames not received in response to an RTS frame.
ACK Failure Count	Count of ACK frames not received when expected.
Received Fragment Count	Count of successfully received MPDU frames of type data or management.
Multicast Received Frame Count	Count of MSDU frames received with the multicast bit set in the destination MAC address.

Field	*Description*
FCS Error Count	Count of FCS errors detected in a received MPDU frame.
Transmitted Frame Count	Count of each successfully transmitted MSDU.
WEP Undecryptable Count	Count of encrypted frames received and the key configuration of the transmitter indicates that the frame should not have been encrypted or that frame was discarded due to the receiving station not implementing the privacy option.

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

```
(Switch) #show wireless ap 00:01:01:02:01:01 radio 1 statistics

MAC Address..................................... 00:01:01:02:01:01
Location........................................ FirstFloor
Radio........................................... 1
WLAN Packets Received........................... 0
WLAN Packets Transmitted........................ 0
WLAN Bytes Received............................. 0
WLAN Bytes Transmitted.......................... 0
WLAN Packets Receive Dropped.................... 0
WLAN Packets Transmit Dropped................... 0
WLAN Bytes Receive Dropped...................... 0
WLAN Bytes Transmit Dropped..................... 0
Fragments Received.............................. 0
Fragments Transmitted........................... 0
Multicast Frames Received....................... 0
Multicast Frames Transmitted.................... 0
Duplicate Frame Count........................... 0
Failed Transmit Count........................... 0
Transmit Retry Count............................ 0
Multiple Retry Count............................ 0
RTS Success Count............................... 0
RTS Failure Count............................... 0
ACK Failure Count............................... 0
FCS Error Count................................. 0
Frames Transmitted.............................. 0
WEP Undecryptable Count......................... 0
```

show wireless ap radio tspec statistics

This command displays TSPEC statistics for each physical radio on a WS managed AP, the managed AP MAC address and radio parameters are required, the command displays a detailed view of the current statistics.

Format `show wireless ap macaddr radio {1-2} tspec statistics`

Mode Privileged EXEC

Field	*Description*
macaddr	WS managed AP MAC address.
1–2	The radio interface on the AP.
MAC Address	The Ethernet address of the WS managed AP.
Location	A location description for the AP, this is the value configured in the valid AP database (either locally or on the RADIUS server).
Radio	Indicates a radio interface on the AP.
Access Category	Identifies the access category to which the following values pertain.
TSPEC Packets Received	Total packets received by the AP on this radio interface for all traffic streams belonging to the designated access category.
TSPEC Packets Transmitted	Total packets transmitted by the AP on this radio interface for all traffic streams belonging to the designated access category.
TSPEC Bytes Received	Total bytes received by the AP on this radio interface for all traffic streams belonging to the designated access category.
TSPEC Bytes Transmitted	Total bytes transmitted by the AP on this radio interface for all traffic streams belonging to the designated access category.

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

```
(Switch) #show wireless ap 00:01:01:02:01:01 radio 1 tspec statistics

MAC Address..................................... 00:01:01:02:01:01
Location........................................ FirstFloor
Radio........................................... 1

Access Category................................. Voice
TSPEC Packets Received.......................... 0
TSPEC Packets Transmitted....................... 0
TSPEC Bytes Received............................ 0
TSPEC Bytes Transmitted......................... 0

Access Category................................. Video
TSPEC Packets Received.......................... 0
TSPEC Packets Transmitted....................... 0
TSPEC Bytes Received............................ 0
TSPEC Bytes Transmitted......................... 0
```

show wireless ap radio vap statistics

This command displays statistics for each VAP on a WS managed AP radio. All parameters are required, and the command displays a detailed view of the current statistics.

Format `show wireless ap macaddr radio {1-2} vap {0-15} statistics`

Mode Privileged EXEC

Field	*Description*
macaddr	WS managed AP MAC address.
1–2	The radio interface on the AP.
0–15	VAP ID.
MAC Address	The Ethernet address of the WS managed AP.
Location	A location description for the AP, this is the value configured in the valid AP database (either locally or on the RADIUS server).
Radio	Indicates a radio interface on the AP.
VAP	Indicates the VAP ID on the radio.
WLAN Packets Received	Total packets received by the AP on this VAP.
WLAN Bytes Received	Total bytes received by the AP on this VAP.
WLAN Packets Transmitted	Total packets transmitted by the AP on this VAP.
WLAN Bytes Transmitted	Total bytes transmitted by the AP on this VAP.
WLAN Packets Receive Dropped	Total receive packets discarded by the AP on this VAP.
WLAN Bytes Received	Total receive bytes discarded by the AP on this VAP.
WLAN Packets Transmitted	Total packets discarded by the AP prior to transmission on this VAP.
WLAN Bytes Transmitted	Total bytes discarded by the AP prior to transmission on this VAP.
Client Association Failures	Number of clients that have been denied association to the VAP.
Client Authentication Failures	Number of clients that have failed authentication to the VAP.

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

```
(Switch) #show wireless ap 00:01:01:02:01:01 radio 1 vap 1 statistics

AP MAC Address.............................. 00:01:01:02:01:01
Location.................................... FirstFloor
Radio....................................... 1
VAP ID...................................... 1
WLAN Packets Received....................... 0
WLAN Packets Transmitted.................... 0
WLAN Bytes Received......................... 0
WLAN Bytes Transmitted...................... 0
WLAN Packets Receive Dropped................ 0
```

```
WLAN Packets Transmit Dropped..................... 0
WLAN Bytes Receive Dropped........................ 0
WLAN Bytes Transmit Dropped....................... 0
Client Association Failures....................... 0
Client Authentication Failures.................... 0
```

show wireless ap radio vap tspec statistics

This command displays TSPEC statistics for each VAP on a WS managed AP radio. All parameters are required, and the command displays a detailed view of the current statistics.

Format `show wireless ap macaddr radio {1-2} vap {0-15} tspec statistics`

Mode Privileged EXEC

Field	*Description*
macaddr	WS managed AP MAC address.
1–2	The radio interface on the AP.
0–15	VAP ID.
MAC Address	The Ethernet address of the WS managed AP.
Location	A location description for the AP, this is the value configured in the valid AP database (either locally or on the RADIUS server).
Radio	Indicates a radio interface on the AP.
VAP	Indicates the VAP ID on the radio.
Access Category	Identifies the access category to which the following values pertain.
TSPEC Packets Received	Total packets received by the AP on this VAP for all traffic streams belonging to the designated access category.
TSPEC Packets Transmitted	Total packets transmitted by the AP on this VAP for all traffic streams belonging to the designated access category.
TSPEC Bytes Received	Total bytes received by the AP on this VAP for all traffic streams belonging to the designated access category.
TSPEC Bytes Transmitted	Total bytes transmitted by the AP on this VAP for all traffic streams belonging to the designated access category.

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

```
(Switch) #show wireless ap 00:01:01:02:01:01 radio 1 vap 1 tspec statistics

AP MAC Address.............................. 00:01:01:02:01:01
Location.................................... FirstFloor
Radio....................................... 1
VAP ID...................................... 1

Access Category............................. Voice
TSPEC Packets Received...................... 0
TSPEC Packets Transmitted................... 0
TSPEC Bytes Received........................ 0
TSPEC Bytes Transmitted..................... 0
```

```
Access Category.............................. Video
TSPEC Packets Received....................... 0
TSPEC Packets Transmitted.................... 0
TSPEC Bytes Received......................... 0
TSPEC Bytes Transmitted...................... 0
```

show wireless ap download

This command displays global configuration and status for an AP code download request. It does not accept any parameters.

Format `show wireless ap download`

Mode Privileged EXEC

Field	*Description*
Image 1File Name	The AP image type 1 filename on the TFTP server.
Image 1File Path	The AP image type 1 file path on the TFTP server.
Image 2File Name	The AP image type 2 filename on the TFTP server.
Image 2 File Path	The AP image 2 filepath on the TFTP server.
Server Address	The TFTP server IP address.
Group Size	If a code download request is for all managed APs, the switch processes the request for one group of APs at a time before starting the next group. The group size indicates the maximum number of APs the switch will send the code download request to at one time.
Download Type	The last download type requested.
Download Status	The global status for the code download request.
Total Count	The total number of managed APs being updated in the current code download request. This may be one AP or the total number of managed APs at the time a code download request is started.
Success Count	Indicates the total number of managed APs that have successfully downloaded their code for the current code download request.
Failure Count	Indicates the total number of managed APs that have failed to download their code for the current code download request.
Abort Count	Indicates the number of APs for which the download was aborted, starting at 0 and incrementing with each aborted download.

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

```
(Routing) #show wireless ap download

image 1 File Name............................ apcode.tar
image 1 File Path............................ ./ap
image 2 File Name............................ apcode2.tar
image 2 File Path............................ ./AP2
Server Address..............................1.1.1.1
Group Size................................... 3
Download Type................................ image1
```

```
Download Status.............................. Not Started
Total Count.................................. 0
Success Count................................ 0
Failure Count................................ 0
Abort Count.................................. 0
```

show wireless ap radio radar status

This command displays radar status for each radio on a WS managed AP. All parameters are required. The radar status is displayed for mode **a** radios only. For **b/g** mode radios, an error is displayed.

Format `show wireless ap macaddr radio {1-2} radar status`

Mode Privileged EXEC

Field	*Description*
macaddr	WS managed AP MAC address
1–2	The radio interface on the AP.
Channel	The list of channels available on the specified radio.
Radar Detection Required	In some regulatory domains, radar detection is required on some channels in the 5 GHz band. If radar detection is required on the channel, the AP uses the 802.11h specification to avoid interference with other wireless devices.
Radar Detected Status	Indicates whether another 802.11 device was detected on the channel.
Last Radar Detected Time	Shows the amount of time that has passed since the device was last detected on the channel.

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

```
(Switching) #show wireless ap 00:22:B0:3A:C1:80 radio 1 radar status

          Radar Detection    Radar Detected     Last Radar
Channel      Required            Status        Detected Time
------- ------------------ ---------------- ----------------
36      No                 No               0d:00:00:00
44      No                 No               0d:00:00:00
52      Yes                No               0d:00:00:00
60      Yes                No               0d:00:00:00
100     Yes                No               0d:00:00:00
108     Yes                No               0d:00:00:00
116     Yes                No               0d:00:00:00
124     Yes                No               0d:00:00:00
132     Yes                No               0d:00:00:00
149     No                 No               0d:00:00:00
157     No                 No               0d:00:00:00
```

Access Point Failure Status Commands

The commands in this section provide views and management of data maintained for access point association and authentication failures.

clear wireless ap failure list

This command deletes all entries from the AP failure list, entries normally age out according to the configured age time. The AP failure list includes entries for all APs that have failed to validate or authenticate to the Wireless Switch.

Format `clear wireless ap failure list`

Mode Privileged EXEC

Example: The following shows an example of the command.

```
(Switch) #clear wireless ap failure list
Are you sure you want to clear the entire AP failure list? (y/n) y
All AP failure entries cleared.

(Switch) #clear wireless ap failure list
Are you sure you want to clear the entire AP failure list? (y/n) n
AP failure entries not cleared.
```

show wireless ap failure status

This command displays summary or detailed data for entries in the AP failure list. Entries are added to the list when the Wireless Switch fails to validate or authenticate an AP.

When acting as a Cluster Controller, the peer Wireless Switch reported AP failures are also displayed. To identify such entries in the summary command display, an * (asterisk) is used alongside the peer Wireless Switch reported AP MAC Address.

Format `show wireless ap [macaddr] failure status`

Mode Privileged EXEC

Field	*Description*
macaddr	The failure AP MAC address.
MAC Address	The Ethernet address of the AP.
IP Address	The network IP address of the AP.
Reporting Switch	Indicates if AP Failure happened with this Wireless Switch or peer Wireless Switch.
Switch MAC Address	The Ethernet address of the Wireless Switch managing the AP.
Switch IP Address	The network IP address of the Wireless Switch managing the AP.

Field	*Description*
Last Failure Type	Indicates the last type of failure that occurred. If the WS supports the Integrated AP image download mode and the AP auto upgrade is enabled, the AP is automatically upgraded upon discovery. However, if no AP image is found on the WS to upgrade the AP, this failure type is reported as 'AP Code Image Not Available'.
Validation Failure Count	The count of association failures for this AP.
Authentication Failure Count	The count of authentication failures for this AP.
Vendor ID	Vendor of the AP software.
Protocol Version	Indicates the protocol version supported by the software on the AP.
Software Version	Indicates the version of software on the AP.
Hardware Type	Hardware platform for the AP.
Age	Time in seconds since failure occurred.

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

On the Cluster Controller, the summary command will display entries in the following format:

```
(Switch) #show wireless ap failure status

    MAC Address
 (*) Peer Managed   IP Address       Last Failure Type           Age
------------------ --------------- ----------------------- ----------------
*00:00:86:00:50:00 192.168.37.74   No Database Entry        0d:00:00:06

On the switch that is not acting as a Cluster Controller the summary command displays entries in
the following format:

(Switch) #show wireless ap failure status

   MAC Address      IP Address       Last Failure Type           Age
----------------- --------------- ----------------------- ----------------
00:00:85:00:50:00 192.168.37.49   No Database Entry        0d:00:02:02
00:00:86:00:50:00 192.168.37.74   No Database Entry        0d:00:00:03


(Switch) #show wireless ap 00:22:B0:3A:C8:40 failure status

MAC address..................................... 00:22:B0:3A:C8:40
IP Address...................................... 10.27.64.163
Reporting Switch................................ Local Switch
Switch MAC Address.............................. 00:02:BC:00:00:77
Switch IP Address............................... 10.27.65.8
Last Failure Type............................... No Database Entry
Validation Failure Count........................ 6
Authentication Failure Count.................... 0
Vendor ID....................................... Broadcom
Protocol Version................................ 2
Software Version................................ 1.0
Hardware Type................................... 0x0000
Age............................................. 0d:00:00:29
```

RF Scan Access Point Status Commands

The commands in this section provide views and management of data maintained for all access points known by the Wireless Switch via RF scan data obtained from the managed access points.

clear wireless ap rf-scan list

This command deletes all entries from the RF scan list; entries normally age out according to the configured age time.

Format `clear wireless ap rf-scan list`

Mode Privileged EXEC

Example: The following shows an example of the command.

```
(Switch) #clear wireless ap rf-scan list
Are you sure you want to clear all RF scan entries? (y/n) y
All RF scan entries cleared.
```

show wireless ap rf-scan status

This command displays summary or detailed data for APs detected via RF scan on the managed APs. If the optional MAC address parameter is specified, detailed data is displayed.

Format `show wireless ap [macaddr] rf-scan status`

Mode Privileged EXEC

Field	*Description*
macaddr	AP MAC address detected in RF scan.
MAC Address	The Ethernet MAC address of the detected AP, this could be a physical radio interface or VAP MAC. For Broadcom APs, this is always a VAP MAC address.
BSSID	Basic Service Set Identifier advertised by the AP in the beacon frames.
SSID	Service Set ID of the network, this is broadcast in the detected beacon frame.
OUI	Vendor name for the MAC address.
Physical Mode	Indicates the 802.11 mode being used on the AP.
Channel	Transmit channel of the AP.

Field	*Description*
Status	Indicates the managed status of the AP, whether this is a valid AP known to the switch or a Rogue on the network. The valid values are: • Managed - The neighbor AP is managed by this switch or another switch within the peer group. The neighbor AP status can be referenced using its base MAC address. • Unknown - The neighbor APs detected in the RF Scan are initially categorized as *Unknown* APs. • Standalone - The AP is managed in standalone mode and configured as a valid AP entry (local or RADIUS). • Rogue - The AP Intrusion Detection function has determined that the AP is posing a threat to the network and categorizes the neighbor AP as *Rogue*.
Age	Time in seconds since this AP was last detected in an RF scan.
The following parameters are displayed only in the detailed status:	
Transmit Rate	Indicates the rate at which the AP is currently transmitting data.
Beacon Period	Beacon interval for the neighbor AP network.
Initial Status	If the AP is not rogue, then initial status is equal to *Status*. For rogue APs, the initial status is the classification prior to this AP becoming rogue. The valid values are: • Managed - The neighbor AP is managed by this switch or another switch within the peer group. The neighbor AP status can be referenced using its base MAC address. • Unknown - The neighbor APs detected in the RF Scan are initially categorized as Unknown APs. • Standalone - The AP is managed in standalone mode and configured as a valid AP entry (local or RADIUS).
AP MAC Address	If status indicates a managed AP, this indicates the base MAC address of the AP.
Radio Interface	If status indicates a managed AP, this indicates the radio interface on the AP.
Discovered Age	Time in seconds since this AP was first detected in an RF scan.
Security Mode	Security used by this AP: Open, WEP, or WPA.
Highest Supported Rate	The highest supported rate advertised by this AP in the beacon frames. An integer value representing the number per 100Kbps.
802.11n Mode	Flag indicating whether this AP supports 802.11n.
Ad Hoc Network	Flag indicating that the beacon frame is received from an Ad hoc network. Possible values are: **false**-Not Ad hoc, **true**-Ad hoc.
Peer Managed AP	Flag indicating this AP is managed by a peer switch. Valid values are: • Locally managed - AP is managed by the local switch. • Peer managed - AP is managed by a peer switch.
Rogue Mitigation	Status indicating whether rogue AP mitigation is in progress for this AP. If mitigation is not in progress then this field displays the reason, which can be one of the following: • Not Required (AP s not rogue) • Already mitigating too many APs. • AP Is operating on an illegal channel. • AP is spoofing valid managed AP MAC address. • AP is Ad hoc.
RRM Support	Indicates whether the radio supports Resource Radio Management (RRM) as defined by the 802.11k standard.

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

```
(Switch) #show wireless ap rf-scan status

                                 Physical                          Discovered
   MAC Address          SSID       Mode   Channel     Status          Age
----------------- --------------- -------- ------- --------------- -----------
00:01:01:02:01:03 Network3        802.11g  6       Managed         3h:28m:11s
00:01:01:02:03:02 Network2        802.11g  6       Managed         3h:28m:14s
00:33:01:02:01:83 Lobby           802.11g  6       Unknown         3h:28m:8s

(Switch) #show wireless ap 00:11:95:A3:7A:C8 rf-scan status

MAC Address..................................... 00:11:95:A3:7A:C8
SSID............................................ Guest Network
OUI............................................. Unknown
Physical Mode................................... 802.11g
Channel......................................... 1
Status.......................................... Rogue
Initial Status.................................. Rogue
Transmit Rate (Mpbs)............................ 1 Mbps
Beacon Period (msecs)........................... 100
Discovered Age.................................. 0d:00:03:01
Age............................................. 0d:00:02:57
Security Mode................................... Open
Highest Supported Rate (per 100Kbps)........... 10
802.11n Mode.................................... Supported
Ad hoc Network.................................. Not Ad hoc
Rogue Mitigation................................ Not Required
Radio Resource Mgmt (RRM) Support.............. Not Supported

(Switch) #
```

show wireless ap rf-scan triangulation

This command displays the signal triangulation status for the specified RF scan entry. Triangulation information is provided to help locate the rogue AP by showing which managed APs detect each device discovered through the RF Scan. Up to six triangulation entries are reported for each AP detected through the RF Scan: three entries by non-sentry APs and three entries by sentry APs. Since an AP may have one radio configured in sentry mode and another radio configured in non-sentry mode, the same AP can appear in both lists. If the AP has not been detected by three APs, then the list may contain zero, one, or two entries.

Format `show wireless ap` *`macaddr`* `rf-scan triangulation`

Mode Privileged EXEC

Field	*Description*
macaddr	AP MAC address detected in RF scan.
Sentry	Identifies whether the AP that detected the entry is in sentry or non-sentry mode.
MAC Address	Shows the MAC address of the AP that detected the RF Scan entry. The address links to the valid AP database.

Field	*Description*
Radio	Identifies the radio on the AP that deleted the RF Scan entry.
RSSI	Shows the received signal strength indicator (RSSI) in terms of percentage for the non-sentry AP. The range is 0, which means the AP is not detected, to 100%.
Signal (dBm)	Received signal strength for the non-sentry AP. The range is -127 dBm to 127 dBm, but most values are expected to be range from -95 dBm to -10 dBm.
Noise (dBm)	Noise reported on the channel by the non-sentry AP.
Age	Time since this AP was last detected in an RF scan.

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

```
(Switch) #show wireless ap 00:02:BC:00:17:D0 rf-scan triangulation

                                  RSSI Signal Noise
  Sentry      MAC Address    Radio (%)  (dBm)  (dBm) Age
---------- ----------------- ----- ---- ------ ----- -----------
Non-Sentry 00:22:B0:3A:C1:80   2     15    -80   -92 0d:15:48:19
```

show wireless ap rf-scan rogue-classification

This command displays the WIDS AP rogue classification test results.

Format `show wireless ap` *`macaddr`* `rf-scan rogue-classification`

Mode Privileged EXEC

Field	*Description*
macaddr	AP MAC address detected in RF scan.
Test ID	Test identifier (WIDSAPROGUEnn).
Cond Detect	Indicates whether this test detected the condition that it is designed to detect. Valid values are **True** or **False**.
MAC Addr (radio)	The Managed AP MAC address and (radio number) that last reported detecting this condition.
Test Config	Indicates whether this test is configured to report rogues. Valid values are **Enable** or **Disable**.
Test Result	Indicates whether this test reported the device as rogue. Valid values are **Rogue** or empty string.
Time Since 1st Report	Time stamp indicating how long ago this test first detected the condition.
Time Since Last Report	Time stamp indicating how long ago this test last detected the condition.

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

```
(Switch) # show wireless ap 00:11:95:A3:7A:C8 rogue-classification

             Cond                        Test    Test   Time Since  Time Since
Test ID      Detect MAC Addr (radio)     Config  Result 1st Report  Last Report
```

```
------------ ------ ------------------- ------- ------ ----------- -----------
WIDSAPROGUE01 True   00:00:00:00:00:11(1) Enable  Rogue  0d:00:00:00 0d:00:00:01
WIDSAPROGUE02 False  00:00:00:00:00:12(2) Disable        0d:00:00:00 0d:00:00:00
WIDSAPROGUE03 True   00:00:00:00:00:13(0) Enable  Rogue  0d:00:00:02 0d:00:00:03
WIDSAPROGUE04 True   00:00:00:00:00:14(1) Enable  Rogue  0d:00:00:04 0d:00:00:05
WIDSAPROGUE05 True   00:00:00:00:00:15(2) Enable  Rogue  0d:00:00:06 0d:00:00:07
WIDSAPROGUE06 True   00:00:00:00:00:16(0) Enable  Rogue  0d:00:01:28 0d:00:01:39
WIDSAPROGUE07 False  00:00:00:00:00:17(1) Enable         0d:00:01:51 0d:00:03:42
WIDSAPROGUE08 False  00:00:00:00:00:18(2) Enable         0d:00:05:33 0d:00:07:24
WIDSAPROGUE09 False  00:00:00:00:00:19(2) Enable         0d:00:09:15 0d:00:11:06
WIDSAPROGUE10 False  00:00:00:00:00:1A(0) Enable         0d:00:12:57 0d:00:14:48
WIDSAPROGUE11 False  00:00:00:00:00:1B(0) Enable         0d:00:00:00 0d:00:00:00

WIDSAPROGUE01..... Administrator configured rogue AP
WIDSAPROGUE02..... Managed SSID from an unknown AP
WIDSAPROGUE03..... Managed SSID from a fake managed AP
WIDSAPROGUE04..... AP without an SSID
WIDSAPROGUE05..... Fake managed AP on an invalid channel
WIDSAPROGUE06..... Managed SSID detected with incorrect security
WIDSAPROGUE07..... Invalid SSID from a managed AP
WIDSAPROGUE08..... AP is operating on an illegal channel
WIDSAPROGUE09..... Standalone AP with unexpected configuration
WIDSAPROGUE10..... Unexpected WDS device detected on network
WIDSAPROGUE11..... Unmanaged AP detected on wired network
```

Client Association Status and Statistics Commands

The commands in this section provide views and management of all status and statistics for wireless clients. In addition to commands to display data from the associated client perspective, this section includes commands to display a view of all clients associated to a specific VAP, and to display a view of all clients associated to a specific SSID.

wireless client disassociate

This command initiates a request to disassociate a client associated to a managed AP specified by the client MAC address. The Wireless Switch will send a message to the appropriate managed AP to force the disassociation.

Format `wireless client disassociate macaddr`

Mode Privileged EXEC

Parameter	*Description*
macaddr	Client MAC address.

show wireless client status

This commands displays summary or detailed data for clients associated to a managed AP. If the Wireless Switch is a Cluster Controller, the command shows all the associated clients in the peer-group. When acting as a Cluster Controller, the peer switch associated clients are displayed with an * (asterisk) before the Client MAC Address in the summary command.

Format `show wireless client [macaddr] status`

Mode Privileged EXEC

Parameter	*Description*
macaddr	Client MAC address.

The command output displays the following information.

Field	*Description*
MAC Address	The Ethernet address of the client station.
Detected IP Address	This is the IPv4 address detected for the clients using ARP snooping.
Tunnel IP Address	This field is blank for all non-tunneled clients. For a tunneled client, this is the assigned tunnel IP address.

Field	*Description*
Associating Switch	Indicates if the client is associated to an AP managed by this Wireless Switch or a peer Wireless Switch.
Switch MAC Address	The Ethernet address of the Wireless Switch associating this client.
Switch IP Address	The network IP address of the Wireless Switch associating this client.
SSID	Indicates the network on which the client is connected.
NETBIOS Name	NETBIOS name of the client.
VAP MAC Address	Indicates the Ethernet MAC address for the managed AP VAP where this client is associated.
Channel	Indicates the operating channel for the client association.
Status	Indicates whether or not the client has associated and/or authenticated. The valid values are: • Associated - The client is currently associated to the managed AP. • Authenticated - The client is currently associated and authenticated to the managed AP. • Disassociated - The client has disassociated from the managed AP. If the client does not roam to another managed AP within the client roam timeout, it will be deleted.
AP MAC Address	This field indicates the base AP Ethernet MAC address for the managed AP.
Location	The descriptive location configured for the managed AP.
Radio	Displays the managed AP radio interface on which the client is associated.
VLAN	If the client is on a VAP using VLAN data forwarding mode, indicates the current assigned VLAN.
User Name	Indicates the user name of clients that have authenticated via 802.1x. Clients on networks with other security modes will not have a user name.
Transmit Data Rate	Indicates the rate at which the client station is currently transmitting data.
802.11n-Capable	For current association, this flag indicates whether the client is capable of 802.11n operation.
STBC Capable	For current association, this flag indicates whether the client is capable of Space Time Block Code (STBC) operation.
Inactive Period	For current association, the period of time that the AP has not seen any traffic for the client.
Age	Indicates the time in seconds since the switch received new status or statistics update for this client.
Network Time	Indicates the time since the client first authenticated with the network.

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

On the Cluster Controller the summary command displays entries in the following format:

```
(DWS-4026) #show wireless client status

    MAC Address
 (*) Peer Managed   VAP MAC Address        SSID        Status    Network Time
------------------ ----------------- ----------------- --------- -------------
*00:0F:B5:86:93:95 00:00:86:00:50:00 l7network         Auth      0d:01:09:52
 00:0F:B5:88:93:95 00:00:88:00:50:00 l7network         Auth      0d:01:09:52
```

```
(DWS-4026) #

On the switch that is not acting as a Cluster Controller the summary command displays entries in
the following format:
(DWS-4026) #show wireless client status

    MAC Address     VAP MAC Address        SSID        Status    Network Time
----------------- ---------------- ---------------- --------- --------------
 00:0F:B5:86:93:95 00:00:86:00:50:00 l7network         Auth      0d:01:09:52

(DWS-4026) #
```

Example: The following shows CLI display output for a particular MAC address:

```
(DWS-4026) #show wireless client 00:14:6c:59:d1:99 status

MAC address..................................... 00:14:6C:59:D1:99
Detected IP Address............................. -----
Detected IP Address............................. -----
VAP MAC Address................................. 00:02:BC:00:17:D0
AP MAC Address.................................. 00:02:BC:00:17:D0
Location.....................................
Radio........................................... 2 - 802.11b/g/n
Associating Switch.............................. Local Switch
Switch MAC Address.............................. 00:FC:E3:90:01:07
Switch IP Address............................... 10.27.64.121
Tunnel IP Address............................... -----
SSID............................................ ALT-VLAN-8
NetBIOS Name.................................... PCRDU-ATSIGLER
Status.......................................... Authenticated
Channel......................................... 1
User Name.....................................
VLAN............................................ 8
Transmit Data Rate.............................. 1 Mbps
802.11n Capable................................. No
STBC Capable.................................... No
Inactive Period................................. 0d:00:00:55
Age............................................. 0d:00:00:04
Network Time.................................... 0d:23:32:51

(DWS-4026) #
```

show wireless client summary

This commands displays a brief summary of clients associated to a managed AP.

If the WS is a Cluster Controller, the command shows all the associated clients in the peer-group.

When acting as Cluster Controller, the peer switch associated clients are displayed with an * (asterisk) before the Client MAC Address in the summary command.

Format	`show wireless client summary`
Mode	Privileged EXEC

The command output displays the following information:

Field	*Description*
MAC Address	The Ethernet address of client station.
IP Address	This is the IPv4 address detected for the clients using ARP snooping.
NetBIOS Name	NetBIOS Name of the client.

Example: On the Cluster Controller the summary command displays entries in the following format:

```
(Switch) #show wireless client summary

    MAC Address
(*) Peer Managed   IP Address        NetBIOS Name
------------------ ----------------- -----------------
*00:0F:B5:86:93:95 8.0.1.29          l7client-01
 00:0F:B5:86:93:96 8.0.1.29          l7client-02

(Switch) #

On the switch that is not acting as a Cluster Controller the summary command displays entries in
the following format:
(Switch) #show wireless client summary

    MAC Address    IP Address        NetBIOS Name
------------------ ----------------- -----------------
 00:0F:B5:86:93:95 8.0.1.29          l7client-01
 00:0F:B5:86:93:96 8.0.1.29          l7client-02
```

show wireless client client-qos status

This command displays detailed client QoS data for clients associated to a managed AP. These are the current operational values in effect for the specified client.

Format `show wireless client macaddr client-qos status`

Mode Privileged EXEC

Field	*Description*
macaddr	Client MAC address.
MAC Address	The Ethernet address of the client station.
SSID	The network on which the client is connected.
Client QoS Operational Status	Indicates whether or not the client is performing client QoS operations. Possible values are **Enabled** or **Disabled**.
Bandwidth Limit Down	The maximum transmission rate limit in bits per second in effect for traffic flowing from the AP to the client. This may differ from the configured value due to rounding. A value of 0 indicates no rate limiting is in effect in this direction.

Field	*Description*
Bandwidth Limit Up	The maximum transmission rate limit in bits per second in effect for traffic flowing from the client to the AP. This may differ from the configured value due to rounding. A value of 0 indicates no rate limiting is in effect in this direction.
Access Control Down	Identifies the access control list in effect for traffic flowing from the AP to the client. Both the ACL type and its name (or number) is displayed. A value of none indicates no access control is in effect in this direction.
Access Control Up	Identifies the access control list in effect for traffic flowing from the client to the AP. Both the ACL type and its name (or number) is displayed. A value of none indicates no access control is in effect in this direction.
Diffserv Policy Down	Identifies the Diffserv policy in effect for traffic flowing from the AP to the client. A value of none indicates no policy is in effect in this direction.
Diffserv Policy Up	Identifies the Diffserv policy in effect for traffic flowing from the client to the AP. A value of none indicates no policy is in effect in this direction.

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

```
(Switch) #show wireless client 00:0F:B5:86:93:95 client-qos status

MAC Address..................................... 00:0F:B5:86:93:95
SSID............................................ l7network
Client QoS Operational Status................... Disabled
Bandwidth Limit Down............................ 0
Bandwidth Limit Up.............................. 0
Access Control Down............................. <none>
Access Control Up............................... <none>
Diffserv Policy Down............................ <none>
Diffserv Policy Up.............................. <none>
```

show wireless client client-qos radius status

This command displays detailed client QoS data for clients associated to a managed AP. These are the configured values successfully obtained from a RADIUS server for the specified client.

Format `show wireless client macaddr client-qos radius status`

Mode Privileged EXEC

Field	*Description*
macaddr	Client MAC address.
MAC Address	The Ethernet address of the client station.
SSID	The network on which the client is connected.
Bandwidth Limit Down	Defines the maximum transmission rate limit in bits per second for traffic flowing from the AP to the client. A value of 0 disables rate limiting in this direction. A value of <none> indicates that this parameter was not obtained from RADIUS for the client.
Bandwidth Limit Up	Defines the maximum transmission rate limit in bits per second for traffic flowing from the client to the AP. A value of 0 disables rate limiting in this direction. A value of <none> indicates that this parameter was not obtained from RADIUS for the client.

Field	*Description*
Access Control Down	Defines the configured access control list to use for traffic flowing from the AP to the client. Both the ACL type and its name (or number) is displayed. A value of <none> indicates that this parameter was not obtained from RADIUS for the client.
Access Control Up	Defines the access control list to use for traffic flowing from the client to the AP. Both the ACL type and its name (or number) is displayed. A value of <none> indicates that this parameter was not obtained from RADIUS for the client.
Diffserv Policy Down	Defines the Diffserv policy to use for traffic flowing from the AP to the client. A value of <none> indicates that this parameter was not obtained from RADIUS for the client.
Diffserv Policy Up	Defines the Diffserv policy to use for traffic flowing from the client to the AP. A value of <none> indicates that this parameter was not obtained from RADIUS for the client..

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

```
(Switch) #show wireless client 00:0F:B5:86:93:95 client-qos radius status

MAC Address..................................... 00:0F:B5:86:93:95
SSID............................................ l7network
Bandwidth Limit Down............................ <none>
Bandwidth Limit Up.............................. <none>
Access Control Down............................. <none>
Access Control Up............................... <none>
Diffserv Policy Down............................ <none>
Diffserv Policy Up.............................. <none>

(Switch) #
```

show wireless client rrm status

This command displays Radio Resource Measurement (RRM) data for clients associated to a managed (or peer-managed) AP. If a MAC address for a particular client is given, the command will list the various RRM capabilities supported by that client. If no address is given, a list of all clients, and whether or not each supports RRM, will be printed.

Format `show wireless client [macaddr] rrm status`

Mode Privileged EXEC

Field	*Description*
macaddr	WS managed AP's client MAC address.
MAC Address	The Ethernet address of the client station.
Radio Resource Mgmt	Indicates if the client supports the Radio Resource Measurement (RRM) portion of the IEEE 802.11k standard.
Location Configuration Requests	Indicates if the client responds to location configuration requests.

Field	*Description*
AP Detection via Beacon Table Report	Indicates whether or not the client can report detected APs through beacon table reports.
Beacon Active Scan Capability	Indicates whether or not the client supports active scan capability.
Beacon Passive Scan Capability	Indicates whether or not the client supports passive scan capability.
Channel Load Measurement	Indicates whether or not the client supports channel load measurement.

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

```
(Switch) #show wireless client rrm status

    MAC Address
 (*) Peer Managed   RRM Supported?
------------------ -----------------
00:12:34:56:78:90     Yes

(Switch) #show wireless client 00:12:34:56:78:90 rrm status

MAC address................................... 00:12:34:56:78:90
Radio Resource Mgmt (RRM)..................... Supported
Location Configuration Requests............... Not Supported
AP Detection via Beacon Table Report.......... Supported
Beacon Active Scan Capability................. Supported
Beacon Passive Scan Capability................ Not Supported
Channel Load Measurement...................... Not Supported
```

show wireless client statistics

This command displays association or session statistics for clients currently associated with a WS managed AP. The session statistics show the cumulative association values if a client roams across managed APs. If no optional parameters are specified, the session statistics are displayed.

Format `show wireless client macaddr statistics [{association | session}]`

Mode Privileged EXEC

Field	*Description*
macaddr	WS managed AP’s client MAC address.
MAC Address	The Ethernet address of the client station.
Packets Received	Total packets received from the client station.
Bytes Received	Total bytes received from the client station.
Packets Transmitted	Total packets transmitted to the client station.

Field	*Description*
Bytes Transmitted	Total bytes transmitted to the client station.
Packets Receive Dropped	Total receive packets from the client station that were discarded by the AP.
Bytes Receive Dropped	Total receive bytes from the client station that were discarded by the AP.
Packets Transmit Dropped	Totals packets discarded by the AP prior to transmission to the client station.
Bytes Transmit Dropped	Total bytes discarded by the AP prior to transmission to the client station.
Duplicate Packets Received	Total duplicate packets received from the client station.
Packet Fragments Received	Total fragmented packets received from the client station.
Packet Fragments Transmitted	Total fragmented packets transmitted to the client station.
Transmit Retry Count	Number of times transmits to the client station succeeded after one or more retries.
Transmit Retry Failed Count	Number of times transmits to the client station failed after one or more retries.
TS Violate Packets Received	Total packets received from the client station that are in violation of traffic stream admission control.
TS Violate Packets Transmitted	Total fragmented packets transmitted to the client station that are in violation of traffic stream admission control.

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

```
(Switch) #show wireless client 00:01:01:10:01:01 statistics

MAC Address..................................... 00:01:01:10:01:01
Packets Received................................ 0
Packets Transmitted............................. 0
Bytes Received.................................. 0
Bytes Transmitted............................... 0
Packets Receive Dropped......................... 0
Packets Transmit Dropped........................ 0
Bytes Receive Dropped........................... 0
Bytes Transmit Dropped.......................... 0
Duplicate Packets Received...................... 0
Packet Fragments Received....................... 0
Packet Fragments Transmitted.................... 0
Transmit Retry Count............................ 0
Failed Retry Count.............................. 0
TS Violate Packets Received..................... 0
TS Violate Packets Transmitted.................. 0

(Switch) #
```

show wireless client neighbor ap status

This command displays all the APs an associated client can see in its RF area; for associated clients this provides a reverse view of the managed AP client neighbor list. It allows you to view where a client may roam based on its neighbor APs.

Format `show wireless client macaddr neighbor ap status`

Mode Privileged EXEC

Field	*Description*
macaddr	Client MAC address.
MAC Address	The Ethernet address of the client station.
AP MAC Address	The base Ethernet address of the WS managed AP.
Location	The configured descriptive location for the managed AP.
Radio	The radio on the managed AP that detected this client as a neighbor.
Discovery Reason	Indicates one or more discovery methods for the neighbor client. One or more of the following abbreviated values may be displayed: • RF Scan (RF) - The client was reported from an RF scan on the radio. Note that client stations are difficult to detect via RF scan, the other methods are more common for client neighbor detection. • Probe Request (Probe) - The managed AP received a probe request from the client. • Associated to Managed AP (Assoc Managed AP) - This neighbor client is associated to another managed AP. • Associated to this AP (Assoc this AP) - The client is associated to this managed AP on the displayed radio. • Associated to Peer AP (Assoc peer AP) - The client is associated to a peer switch managed AP. • Ad Hoc Rogue (Ad Hoc) - The client was detected as part of an ad hoc network.

show wireless client tspec status

This command displays detailed data for clients associated to a managed AP. Information is only displayed if the client has one or more admitted TSPECs.

Format `show wireless client [macaddr] tspec status`

Mode Privileged EXEC

Field	*Description*
macaddr	Client MAC address.
MAC Address	The Ethernet address of the client station.
Detected IP Address	This is the IPv4 address detected for the clients using ARP snooping.

Field	*Description*
Tunnel IP Address	This field is blank for all non-tunneled clients. For a tunneled client, this is the assigned tunnel IP address.
VAP MAC Address	Indicates the Ethernet MAC address for the managed AP VAP where this client is associated.
AP MAC Address	This field indicates the base AP Ethernet MAC address for the managed AP.
Location	The descriptive location configured for the managed AP.
Radio	Displays the managed AP radio interface on which the client is associated.
Associating Switch	Indicates if the client is associated to AP managed by this WS or peer WS.
Switch MAC Address	The Ethernet address of the WS associating this client.
Switch IP Address	The network IP address of the WS associating this client.
Tunnel IP Address	This field is blank for all non-tunneled clients. For a tunneled client, this is the assigned tunnel IP address.
SSID	Indicates the network on which the client is connected.
Traffic Stream Identifier (TID)	The identifying number specified in the TSPEC to which the traffic stream corresponds.
Access Category	The access category to which the traffic stream corresponds.
Direction	The direction of the traffic stream as indicated in the TSPEC. This is one of Uplink, Downlink, or Bidirectional.
User Priority	The user priority indicated in the TSPEC, which identifies the traffic stream for the client. This value translates directly to an access category.
Medium Time	The amount of wireless medium time allocated to the client for this traffic stream. It was calculated by the access point based on parameters contained in the TSPEC, and is represented in units of 32 microseconds per second (usec/sec).
Excess Usage Events	Indicates the number of times the client has appreciably exceeded the medium time established for its TSPEC. Some allowance for minor overages is allowed, but this value represents excess usage of wireless bandwidth on a repeated basis.
Roaming Client	For current association, flag indicating whether this traffic stream was established by a wireless client that was considered to be a roaming client.

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

```
(Switch) #show wireless client 00:0F:B5:86:93:95 tspec status

MAC Address..................................... 00:0F:B5:86:93:95
Detected IP Address............................. 192.168.37.110
VAP MAC Address................................. 00:00:86:00:50:00
AP MAC Address.................................. 00:00:86:00:50:00
Location........................................ ap-6
Radio........................................... 1 - 802.11g
Managing Switch................................. Local Switch
Switch MAC Address.............................. 00:11:88:2B:41:01
Switch IP Address............................... 192.168.37.60
Tunnel IP Address............................... -----
SSID............................................ l7network

Traffic Stream Identifier (TID)................ 1
```

```
Access Category.............................. Video
Direction.................................... Bidirectional
User Priority................................ 4
Medium Time.................................. 860
Excess Usage Events.......................... 0
Roaming Client............................... No

Traffic Stream Identifier (TID)............... 2
Access Category.............................. Voice
Direction.................................... Bidirectional
User Priority................................ 6
Medium Time.................................. 3419
Excess Usage Events.......................... 0
Roaming Client............................... No\
```

show wireless client tspec statistics

This command displays TSPEC statistics for clients currently associated with a WS managed AP. These are effectively association statistics, since a TSPEC is not maintained across a client session.

Information is only displayed if the client has one or more admitted TSPECs.

Format `show wireless client macaddr tspec statistics`

Mode Privileged EXEC

Field	*Description*
macaddr	Client MAC address.
MAC Address	The Ethernet address of the client station.
Traffic Stream Identifier (TID)	The identifying number specified in the TSPEC to which the traffic stream corresponds.
Access Category	The access category to which the traffic stream corresponds.
Direction	The direction of the traffic stream as indicated in the TSPEC. This is one of Uplink, Downlink, or Bidirectional.
TSPEC Packets Received	Total packets received from the client station for this traffic stream for the specified access category.
TSPEC Packets Transmitted	Total packets transmitted to the client station for this traffic stream for the specified access category.
TSPEC Bytes Received	Total bytes received from the client station for this traffic stream for the specified access category.
TSPEC Bytes Transmitted	Total bytes transmitted to the client station for this traffic stream for the specified access category.

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

```
(Switch) #show wireless client 00:0F:B5:86:93:95 tspec statistics

MAC Address.................................. 00:0F:B5:86:93:95
```

```
Traffic Stream Identifier (TID)..... 1
Access Category..................... Video
Direction........................... Bidirectional
TSPEC Packets Received.............. 0
TSPEC Packets Transmitted........... 0
TSPEC Bytes Received................ 0
TSPEC Bytes Transmitted............. 0

Traffic Stream Identifier (TID)..... 2
Access Category..................... Voice
Direction........................... Uplink
TSPEC Packets Received.............. 0
TSPEC Packets Transmitted........... 0
TSPEC Bytes Received................ 0
TSPEC Bytes Transmitted............. 0
```

show wireless vap client status

This command displays summary data for all managed AP VAPs with associated clients. If the optional VAP MAC address is specified, the display will only show clients associated to the specific managed AP VAP.

Format `show wireless vap [macaddr] client status`

Mode Privileged EXEC

Field	*Description*
macaddr	WS managed AP VAP MAC address.
VAP MAC Address	Indicates the Ethernet MAC address for the managed AP VAP where this client is associated.
MAC Address	The Ethernet address of client station.

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

```
(Switch) #show wireless vap 00:02:03:04:05:08 client status
VAP MAC Address    Client MAC Address
-----------------  ------------------
00:02:03:04:05:08  00:02:03:04:05:06
                   00:02:03:04:05:07
```

show wireless ssid client status

This command displays summary data for all managed SSIDs with associated clients. If the optional SSID string is specified, the display will only show clients associated to that network. The SSID/network may exist on one or more managed AP VAPs.

Format `show wireless ssid [ssid] client status`

Mode Privileged EXEC

Field	*Description*
ssid	Service Set Identifier for the network.
MAC Address	The Ethernet address of the client station.
SSID	Indicates the network on which the client is connected.

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

```
(Switch) #show wireless ssid client status

                                   Client
             SSID                 MAC Address    Channel    Status
------------------------------ ----------------- ------- --------------------
Network2                       00:01:01:16:01:01 44      Authenticated
                               00:01:01:20:01:01 44      Authenticated
                               00:01:01:22:01:01 44      Authenticated
Network3                       00:01:01:10:01:01 6       Associated
                               00:01:01:14:01:01 6       Authenticated

(Switch) #
```

show wireless switch client status

This command displays summary data for all switches with associated clients. If the Wireless Switch is a Cluster Controller, then this command shows all clients associated to the APs managed by all the peer switches. For non-Cluster Controller switches, only clients managed by the local switches are displayed.

Format `show wireless switch [ipaddr] client status`

Mode Privileged EXEC

Field	*Description*
ipaddr	IP address of the switch in the wireless system.
IP Address	IP address of the Wireless Switch or any peer switch in the wireless system.
MAC Address	The Ethernet address of the client station.

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

If a network consists of two switches 192.168.37.60 and 192.168.37.61 respectively and former is the Cluster Controller, this command works differently at Cluster Controller and non-Cluster Controller as follows.

On the Cluster Controller, it displays entries in the following format:

```
 (Switch) #show wireless switch client status

                                    Client
       Switch IP Address            MAC Address     Channel       Status
------------------------------ -----------------  ------- --------------------
         192.168.37.60           00.0F.B5.86.93.95    1         Authenticated
                                 00:14:C2:0C:47:6D    1         Authenticated
         192.168.37.61           00.0F.B5.86.93.85    6         Authenticated
                                 00:14:C2:0C:47:1D   11         Authenticated

(Switch) #show wireless switch 192.168.37.60 client status

                                    Client
       Switch IP Address            MAC Address     Channel       Status
------------------------------ -----------------  ------- --------------------
         192.168.37.60           00.0F.B5.86.93.95    1         Authenticated
                                 00:14:C2:0C:47:6D    1         Authenticated

(Switch) #show wireless switch 192.168.37.61 client status

                                    Client
       Switch IP Address            MAC Address     Channel       Status
------------------------------ -----------------  ------- --------------------
         192.168.37.61           00.0F.B5.86.93.85    6         Authenticated
                                 00:14:C2:0C:47:1D   11         Authenticated
```

On the switch that is not acting as a Cluster Controller the summary command displays entries in the following format:

```
(Switch) #show wireless switch client status

                                    Client
       Switch IP Address            MAC Address     Channel       Status
------------------------------ -----------------  ------- --------------------
         192.168.37.61           00.0F.B5.86.93.85    6         Authenticated
                                 00:14:C2:0C:47:1D   11         Authenticated

(Switch) #show wireless switch 192.168.37.60 client status
Error! Only Cluster Controller can display the peer switch associated client status.

(Switch) #show wireless switch 192.168.37.61 client status
                                    Client
       Switch IP Address            MAC Address     Channel       Status
------------------------------ -----------------  ------- --------------------
         192.168.37.61           00.0F.B5.86.93.85    6         Authenticated
                                 00:14:C2:0C:47:1D   11         Authenticated
```

Client Failure and Ad Hoc Status Commands

The commands in this section provide views and management of data maintained for wireless client association and authentication failures.

clear wireless client failure list

This command deletes all entries from the client failure list. Entries normally age out according to the configured age time.

Format `clear wireless client failure list`

Mode Privileged EXEC

Example: The following shows an example of the command.

```
(Switch) #clear wireless client failure list
Are you sure you want to clear all client failure entries? (y/n) y
All client failure entries cleared.
```

clear wireless client adhoc list

This command deletes all entries from the Ad Hoc client list. Entries normally age out according to the configured age time.

Format `clear wireless client adhoc list`

Mode Privileged EXEC

show wireless client failure status

This command displays the client failure status parameters.

Format `show wireless client [macaddr] failure status`

Mode Privileged EXEC

Field	*Description*
macaddr	Client MAC address.
MAC Address	The Ethernet address of the client.
VAP MAC Address	The managed AP VAP Ethernet MAC address on which the client attempted to associate and/or authenticate.
SSID	The network SSID on which the client attempted to associate and/or authenticate.
Last Failure Type	Indicates the last type of failure that occurred.

Field	*Description*
Authentication Failure Count	Count of authentication failures for this client.
Association Failure Count	Count of association failures for this client.
Age	Time since failure occurred.

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

```
(Switch) #show wireless client failure status

                                                                Failure
   MAC Address     VAP MAC Address           SSID               Type      Age
----------------- ----------------- ---------------------- ------- -----------
00:01:21:18:01:01 00:01:01:02:02:02 Network2                Auth    0h:1m:38s
00:01:32:18:01:01 00:01:01:02:01:03 Network3                Assoc   0h:1m:44s

(Switch) #
(Switch) #show wireless client 00:01:21:18:01:01 failure status

MAC Address..................................... 00:01:21:18:01:01
VAP MAC Address................................. 00:01:01:02:02:02
SSID............................................ Network2
Last Failure Type............................... Authentication
Association Failure Count....................... 0
Authentication Failure Count.................... 2
Age............................................. 0h:3m:14s

(Switch) #
```

show wireless client adhoc status

This command displays summary or detailed data for Ad Hoc clients detected on the network by a managed AP.

Format `show wireless client [macaddr] adhoc status`

Mode Privileged EXEC

Field	*Description*
macaddr	Client MAC address.
MAC Address	The Ethernet address of the client. If the Detection Mode is Beacon, then the client is represented as an AP in the RF Scan database and the Neighbor AP List. If the Detection Mode is Data Frame, then the client information is in the Neighbor Client List.
AP MAC Address	The base Ethernet MAC Address of the managed AP which detected the client.
Location	The configured descriptive location for the managed AP.
Radio	The radio interface on the AP that detected the ad hoc device.
Detection Mode	The mechanism of detecting this Ad Hoc device. The possible values are *Beacon Frame* or *Data Frame*.
Age	Time in seconds since the last detection of the ad hoc network.

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

```
(Switch) #show wireless client adhoc status

   MAC Address     AP MAC Address    Location   Radio Detection Mode     Age
----------------- ----------------- ----------- ----- -------------- ----------
00:01:01:30:01:01 00:01:01:02:01:01 FirstFloor  1     Beacon Frame   3h:45m:4s
00:01:01:42:01:01 00:01:01:02:03:01 Eng         1     Beacon Frame   3h:44m:59s
00:01:01:45:01:01 00:01:01:02:01:01 FirstFloor  1     Beacon Frame   3h:45m:2s

(Switch) #
```

WIDS Access Point RF Security Commands

The commands in this section provide views and management of data maintained for the Wireless Intrusion Detection System (WIDS) for RF Security.

wids-security admin-config-rogue

(Administrator-configured rogue detection.) If the local database indicates that an AP is rogue, use this command to report the AP as rogue in the RF Scan.

Default	Enable
Format	`wids-security admin-config-rogue`
Mode	Wireless Config

wids-security ap-chan-illegal

(AP is operating on an illegal channel Rogue Detection.) Use this command to enable rogue reporting for AP's operating on an illegal channel.

Default	Enable
Format	`wids-security ap-chan-illegal`
Mode	Wireless Config

no wids-security ap-chan-illegal

Use this command to disable the mode to report APs operating on an illegal channel.

Format	`no wids-security ap-chan-illegal`
Mode	Wireless Config

wids-security ap-de-auth-attack

(AP de-authentication attack.) Use this command to enable the AP de-authentication attack.

Default Disable
Format `wids-security ap-de-auth-attack`
Mode Wireless Config

no wids-security ap-de-auth-attack

Use this command to disable the AP de-authentication attack.

Format `no wids-security ap-de-auth-attack`
Mode Wireless Config

wids-security fakeman-ap-managed-ssid

Use this command to enable Rogue reporting for fake managed AP's detected with a managed SSID.

Default Enable
Format `wids-security fakeman-ap-managed-ssid`
Mode Wireless Config

no wids-security fakeman-ap-managed-ssid

Use this command to disable Rogue reporting for fake managed AP's detected with a managed SSID.

Format `no wids-security fakeman-ap-managed-ssid`
Mode Wireless Config

wids-security fakeman-ap-chan-invalid

(Beacon received from a fake managed AP on an invalid channel Rogue Detection.) Use this command to enable rogue reporting for fake managed APs detected with an invalid channel.

Default Enable
Format `wids-security fakeman-ap-chan-invalid`
Mode Wireless Config

no wids-security fakeman-ap-chan-invalid

Use this command to disable Rogue reporting for fake managed AP's detected with an invalid channel.

Format `no wids-security fakeman-ap-chan-invalid`

Mode Wireless Config

wids-security fakeman-ap-no ssid

(Beacon received from fake managed AP without SSID rogue detection.) Use this command to enable rogue reporting for fake managed AP's detected with no SSID.

Default Enable

Format `wids-security fakeman-ap-no-ssid`

Mode Wireless Config

no wids-security fakeman-ap-no ssid

Use this command to disable rogue reporting for fake managed APs detected with an invalid channel.

Format `no wids-security fakeman-ap-no ssid`

Mode Wireless Config

wids-security managed-ap-no-ssid

(Beacon received from a fake managed AP without SSID Rogue Detection). Use this command to enable rogue reporting for fake managed AP's detected with no SSID.

Default Enable

Format `wids-security managed-ap-no-ssid`

Mode Wireless Config

no wids-security managed-ap-no-ssid

Use this command to disable the mode to report fake managed AP's detected with no SSID.

Format `no wids-security managed-ap-no-ssid`

Mode Wireless Config

wids-security managed-ap-chan-invalid

(Beacon received from a fake managed AP on an invalid channel Rogue Detection). Use this command to enable rogue reporting for fake managed AP's detected with an invalid channel.

Default Enable

Format `wids-security managed-ap-chan-invalid`

Mode Wireless Config

no wids-security managed-ap-chan-invalid

Use this command to disable the mode to report fake managed AP's detected with an invalid channel.

Format `no wids-security managed-ap-chan-invalid`

Mode Wireless Config

wids-security managed-ap-ssid-invalid

(Invalid SSID received from a managed AP Rogue Detection.) Use this command to enable rogue reporting for managed AP's detected with an invalid SSID.

Default Enable

Format `wids-security managed-ap-ssid-invalid`

Mode Wireless Config

no wids-security managed-ap-ssid-invalid

Use this command to disable the mode to report managed APs detected with an invalid SSID.

Format `no wids-security managed-ap-ssid-invalid`

Mode Wireless Config

wids-security managed-ssid-secu-bad

(Managed SSID detected with incorrect security configuration Rogue Detection). Use this command to enable rogue reporting for AP's detected with managed SSID's and an invalid security configuration.

Default Enable

Format `wids-security managed-ssid-secu-bad`

Mode Wireless Config

no wids-security managed-ssid-secu-bad

Use this command to disable the mode to report AP's detected with managed SSID's and an invalid security configuration.

Format `no wids-security managed-ssid-secu-bad`

Mode Wireless Config

wids-security rogue-det-trap-interval

(Rogue-detected trap interval.) Use this command to set the interval in seconds between transmissions of the trap telling you that rogues are present in the RF Scan database.

Default 300

Format `wids-security rogue-det-trap-interval {0 | 60-3600}`

Mode Wireless Config

Parameter	*Description*
0, 60–3600	The interval in seconds between transmissions of the trap telling you that rogues are present in the RF Scan database. The trap interval range is 60–3600 seconds. A configured value of 0 disables the trap from being set.

no wids-security rogue-det-trap-interval

Use this command to restore the rogue detected trap interval to its default value.

Format `no wids-security rogue-det-trap-interval`

Mode Wireless Config

wids-security standalone-cfg-invalid

(Standalone AP is operating with unexpected channel, SSID, security, or WIDS mode Rogue Detection.) Use this command to enable rogue reporting for standalone APs operating with unexpected channel, SSID, security, or WIDS mode.

Default Enable

Format `wids-security standalone-cfg-invalid`

Mode Wireless Config

no wids-security standalone-cfg-invalid

Use this command to disable the mode to report standalone AP's operating with unexpected channel, SSID, security, or WIDS mode.

Format `no wids-security standalone-cfg-invalid`

Mode Wireless Config

wids-security unknown-ap-managed-ssid

(Managed SSID received from unknown AP Rogue Detection.) Use this command to enable rogue reporting for unknown rogue APs detected with a managed SSID.

Default Enable

Format `wids-security unknown-ap-managed-ssid`

Mode Wireless Config

no wids-security unknown-ap-managed-ssid

Use this command to disable reporting unknown rogue APs detected with a managed SSID.

Format `no wids-security unknown-ap-managed-ssid`

Mode Wireless Config

wids-security unmanaged-ap-wired

(Unmanaged AP is detected on a wired network Rogue Detection.) Use this command to enable rogue reporting for detection of unmanaged AP's on a wired network.

Default Enable

Format `wids-security unmanaged-ap-wired`

Mode Wireless Config

no wids-security unmanaged-ap-wired

Use this command to disable the mode to report unmanaged APs on a wired network.

Format `no wids-security unmanaged-ap-wired`

Mode Wireless Config

wids-security wds-device-unexpected

(Unexpected WDS device is detected on the network Rogue Detection.) Use this command to enable rogue reporting for detection of unexpected WDS devices.

Default Enable

Format `wids-security wds-device-unexpected`

Mode Wireless Config

no wids-security wds-device-unexpected

Use this command to disable the mode to report detection of unexpected WDS devices.

Format `no wids-security wds-device-unexpected`

Mode Wireless Config

wids-security wired-detection-interval

(Minimum wired detection interval.) Use this command to set the minimum number of seconds that the AP waits before starting a new wired network detection cycle.

Default 60

Format `wids-security wired-detection-interval interval`

Mode Wireless Config

Parameter	*Description*
interval	Minimum number of seconds that the AP waits before starting a new wired network detection cycle. The range is 1–3600 seconds. A value of zero (0) disables wired detection.

no wids-security wired-detection-interval

This command restores the minimum wired detection interval to its default value.

Format `no wids-security wired-detection-interval`

Mode Wireless Config

show wireless wids-security

This command displays the configured wireless WIDS security settings.

Format `show wireless wids-security`

Mode Privileged EXEC

Field	*Description*
Rogue - admin configured Rogue APs	If the local database indicates that the AP is rogue, then reports the AP as rogue in the RF Scan.
Rogue - APs on an illegal channel	Enable or disable rogue reporting for APs operating on an illegal channel.
Rogue - fake managed AP/ invalid channel	Enable or disable rogue reporting for fake managed APs on an invalid channel.
Rogue - fake managed AP/no SSID	Enable or disable rogue reporting for fake managed APs without an SSID.
Rogue - managed AP/invalid SSID	Enable or disable rogue reporting for a managed AP with an invalid SSID.
Rogue - managed SSID/ invalid security	Enable or disable rogue reporting for APs with a managed SSID and an incorrect security configuration.
Rogue - standalone AP/ unexpected config	Enable or disable rogue reporting for standalone APs operating with unexpected channel, security, or WIDS mode.
Rogue - unknown AP/ managed SSID	Enable or disable rogue reporting for unknown rogue APs detected with a managed SSID.
Rogue - unmanaged AP on a wired network	Enable or disable rogue reporting for unmanaged APs on a wired network.
Rogue - unexpected WDS devices	Enable or disable rogue reporting for unexpected WDS devices detected on the network.
Rogue detected trap interval	The interval in seconds between transmissions of the trap telling the administrator that rogues are present in the RF Scan database.
Wired network detection interval	Minimum number of seconds that the AP waits before starting a new wired network detection cycle.
AP De-authentication Attack	Enable or disable the AP De-authentication attack.

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

```
(Switch) # show wireless wids-security

Rogue - admin configured Rogue AP's..... Enable
Rogue - AP's on an illegal channel..... Enable
Rogue - fake managed AP / invalid channel..... Enable
Rogue - fake managed AP / no SSID..... Enable
Rogue - managed AP / invalid SSID..... Enable
Rogue - managed SSID / invalid security..... Enable
Rogue - standalone AP / unexpected config..... Enable
Rogue - unknown AP / managed SSID..... Enable
Rogue - unmanaged AP on a wired network..... Enable
```

```
Rogue - unexpected WDS devices.................. Enable
Rogue detected trap interval.................... 60 seconds
Wired network detection interval................ 60 seconds
AP De-Authentication Attack..................... Disable
```

show wireless wids-security rogue-classification

This command displays the WIDS AP rogue classification test results.

Format `show wireless wids-security macaddr rogue-classification`

Mode Privileged EXEC

Field	*Description*
macaddr	MAC address of the rogue AP.
TestID	Test identifier (WIDSAPROGUEnn).
Detect	Indicates whether this test detected the condition that it is designed to detect. Possible values are **True** or **False**.
MAC Addr (radio)	The Managed AP MAC address and (radio number) last reported detecting this condition.
Config	Indicates whether this test is configured to report rogues. Possible values are **Enable** or **Disable**.
Result	Indicates whether this test reported the device as rogue (Possible values are **Rogue** or empty string.)
1st Report	Time stamp indicating how long ago this test first detected the condition.
Last Report	Time stamp indicating how long ago this test last detected the condition.

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

```
(Switch) # show wireless wids-security 00:11:95:A3:7A:C8 rogue-classification

Test ID       Detect   MAC Addr (radio)   Config  Result 1st Report  Last Report
------------- ------ -------------------- ------- ------ ----------- -----------
WIDSAPROGUE01 True   00:00:00:00:00:11(1) Enable  Rogue  0d:00:00:00 0d:00:00:01
WIDSAPROGUE02 False  00:00:00:00:00:12(2) Disable        0d:00:00:00 0d:00:00:00
WIDSAPROGUE03 True   00:00:00:00:00:13(0) Enable  Rogue  0d:00:00:02 0d:00:00:03
WIDSAPROGUE04 True   00:00:00:00:00:14(1) Enable  Rogue  0d:00:00:04 0d:00:00:05
WIDSAPROGUE05 True   00:00:00:00:00:15(2) Enable  Rogue  0d:00:00:06 0d:00:00:07
WIDSAPROGUE06 True   00:00:00:00:00:16(0) Enable  Rogue  0d:00:01:28 0d:00:01:39
WIDSAPROGUE07 False  00:00:00:00:00:17(1) Enable         0d:00:01:51 0d:00:03:42
WIDSAPROGUE08 False  00:00:00:00:00:18(2) Enable         0d:00:05:33 0d:00:07:24
WIDSAPROGUE09 False  00:00:00:00:00:19(2) Enable         0d:00:09:15 0d:00:11:06
WIDSAPROGUE10 False  00:00:00:00:00:1A(0) Enable         0d:00:12:57 0d:00:14:48

To see test descriptions use show wireless wids-security rogue-test-descriptions.
```

show wireless wids-security rogue-test-descriptions

This command displays the WIDS AP rogue classification test identifier descriptions.

Format `show wireless wids-security rogue-test-descriptions`

Mode Privileged EXEC

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

```
(Switch) # show wireless wids-security rogue-test-descriptions

WIDSAPROGUE01..................... Administrator configured rogue AP
WIDSAPROGUE02..................... Managed SSID from an unknown AP
WIDSAPROGUE03..................... Managed SSID from a fake managed AP
WIDSAPROGUE04..................... AP without an SSID
WIDSAPROGUE05..................... Fake managed AP on an invalid channel
WIDSAPROGUE06..................... Managed SSID detected with incorrect security
WIDSAPROGUE07..................... Invalid SSID from a managed AP
WIDSAPROGUE08..................... AP is operating on an illegal channel
WIDSAPROGUE09..................... Standalone AP with unexpected configuration
WIDSAPROGUE10..................... Unexpected WDS device detected on network
WIDSAPROGUE11..................... Unmanaged AP detected on wired network
```

show wireless wids-security de-authentication

This command displays information about APs against which the Cluster Controller initiated a de-authentication attack.

Format `show wireless wids-security de-authentication`

Mode Privileged EXEC

Field	*Description*
BSSID	BSSID of the AP against which the attack is launched.
Channel	Channel on which the rogue AP is operating.
Attack Time	Time since attack started on this AP.
Age	Time since RF Scan report about this AP.

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

```
(Switch) # show wireless wids-security de-authentication

      BSSID       Channel Attack Time     Age
----------------- ------- ----------- -----------
00:02:BB:00:0A:01   3     0d:00:01:51 0d:00:01:28
00:02:BB:00:14:02   6     0d:00:03:42 0d:00:02:56
00:02:BB:00:1E:03   9     0d:00:05:33 0d:00:04:24
00:02:BB:00:28:04   12    0d:00:07:24 0d:00:05:52
00:02:BB:00:32:05   15    0d:00:09:15 0d:00:07:20
00:02:BB:00:3C:06   18    0d:00:11:06 0d:00:08:48
```

```
00:02:BB:00:46:07   21    0d:00:12:57 0d:00:10:16
00:02:BB:00:50:08   24    0d:00:14:48 0d:00:11:44
00:02:BB:00:5A:09   27    0d:00:16:39 0d:00:13:12
00:02:BB:00:64:0A   30    0d:00:18:30 0d:00:14:40
00:02:BB:00:6E:0B   33    0d:00:20:21 0d:00:16:08
00:02:BB:00:78:0C   36    0d:00:22:12 0d:00:17:36
00:02:BB:00:82:0D   39    0d:00:24:03 0d:00:19:04
00:02:BB:00:8C:0E   42    0d:00:25:54 0d:00:20:32
00:02:BB:00:96:0F   45    0d:00:27:45 0d:00:22:00
00:02:BB:00:A0:10   48    0d:00:29:36 0d:00:23:28
```

Detected Clients Database Commands

This section provides status and configuration commands for the detected client database.

wids-security client rogue-det-trap-interval

Use this command to set the interval in seconds between transmissions of the trap telling you that rogue clients are present in the Detected Clients Database.

Default 60

Format `wids-security client rogue-det-trap-interval {0-3600}`

Mode Wireless Config

Parameter	*Description*
0–3600	Interval in seconds between transmissions of the trap. The range is 0–3600 seconds. A configured value of 0 disables the trap from being sent.

no wids-security client rogue-det-trap-interval

Use this command to restore the rogue detection trap interval to its default value, 60.

Format `no wids-security client rogue-det-trap-interval`

Mode Wireless Config

Example: The following shows an example of the command.

```
(Switch) # wids-security client rogue-det-trap-interval 60  ?
<cr>    Press Enter to execute the command.

(Switch) # no wids-security client rogue-det-trap-interval ?
<cr>    Press Enter to execute the command.
```

wids-security client known-client-database

Use this command to enable the test which marks the client as a rogue if it is not in the Known Clients database.

Default Disable

Format `wids-security client known-client-database`

Mode Wireless Config

no wids-security client known-client-database

Use this command to disable the check for the client in the Known Clients database.

Format `no wids-security client known-client-database`

Mode Wireless Config

wids-security client configured-auth-rate

Use this command to enable the test which marks the client as rogue if it exceeds the configured rate for transmitting 802.11 authentication requests.

Default Enable

Format `wids-security client configured-auth-rate`

Mode Wireless Config

no wids-security client configured-auth-rate

Use this command to disable the test for checking if the client exceeds the configured rate for transmitting 802.11 authentication requests.

Format `no wids-security client configured-auth-rate`

Mode Wireless Config

wids-security client configured-probe-rate

Use this command to enable the test which marks the client as rogue if it exceeds the configured rate for transmitting probe requests.

Default Enable

Format `wids-security client configured-probe-rate`

Mode Wireless Config

no wids-security client configured-probe-rate

Use this command to disable the test for checking if the client exceeds the configured rate for transmitting probe requests.

Format `no wids-security client configured-probe-rate`

Mode Wireless Config

wids-security client configured-deauth-rate

Use this command to enable the test which marks the client as rogue if it exceeds the configured rate for transmitting 802.11 de-authentication requests.

Default Enable

Format `wids-security client configured-deauth-rate`

Mode Wireless Config

no wids-security client configured-deauth-rate

Use this command to disable the test for checking if the client exceeds the configured rate for transmitting 802.11 de-authentication requests.

Format `no wids-security client configured-deauth-rate`

Mode Wireless Config

wids-security client max-auth-failure

Use this command to enable the test which marks the client as rogue if it exceeds the maximum number of authentication failures.

Default Enable

Format `wids-security client max-auth-failure`

Mode Wireless Config

no wids-security client max-auth-failure

Use this command to disable the test for checking if the client has exceeded the configured rate for maximum authentication failures.

Format `no wids-security client max-auth-failure`

Mode Wireless Config

wids-security client auth-with-unknown-ap

Use this command to enable the test to check if a known client is authenticated with an unknown AP. If yes, then the client is marked as a rogue.

Default Enable

Format `wids-security client auth-with-unknown-ap`

Mode Wireless Config

no wids-security client auth-with-unknown-ap

Use this command to disable the test for checking if the client is authenticated with an unknown AP.

Format `no wids-security client auth-with-unknown-ap`

Mode Wireless Config

wids-security client threat-mitigation

Use this command to enable the transmission of de-authentication messages to known clients associated with unknown APs. The *Known Client* test must also be enabled order for the mitigation to take place.

Default Disable

Format `wids-security client threat-mitigation`

Mode Wireless Config

no wids-security client threat-mitigation

Use this command to disable the test for Client Threat Mitigation.

Format `no wids-security client threat-mitigation`

Mode Wireless Config

wids-security client threshold-value-deauth

Use this command to configure the maximum number of de-authentication messages which a switch can receive during the threshold interval.

Default 10

Format `wids-security client threshold-value-deauth {1-99999}`

Mode Wireless Config

Parameter	*Description*
1–99999	Range of the threshold value.

no wids-security client threshold-value-deauth

Use this command to set the threshold-value for de-authentication messages to the default.

Format `no wids-security client threshold-value-deauth`

Mode Wireless Config

wids-security client threshold-interval-deauth

Use this command to configure the threshold interval for counting the de-authentication messages.

Default 60

Format `wids-security client threshold-interval-deauth {1-3600}`

Mode Wireless Config

Parameter	*Description*
1–3600	Range of the threshold value.

no wids-security client threshold-interval-deauth

Use this command to set the threshold value for the de-authentication interval to its default.

Format `no wids-security client threshold-interval-deauth`

Mode Wireless Config

wids-security client threshold-value-auth

Use this command to configure the maximum number of authentication messages a switch can receive during the threshold interval.

Default 10

Format `wids-security client threshold-value-auth {1-99999}`

Mode Wireless Config

Parameter	*Description*
1–99999	The range of the threshold value.

no wids-security client threshold-value-auth

Use this command to set the threshold value for authentication messages to its default.

Format `no wids-security client threshold-value-auth`

Mode Wireless Config

wids-security client threshold-interval-auth

Use this command to configure the threshold interval for counting the authentication messages at the switch.

Default 60

Format `wids-security client threshold-interval-auth {1-3600}`

Mode Wireless Config

no wids-security client threshold-interval-auth

Use this command to set the threshold value for the authentication interval to its default.

Format `no wids-security client threshold-interval-auth`

Mode Wireless Config

wids-security client threshold-value-probe

Use this command to configure the maximum number of probe messages a switch can receive during the threshold interval.

Default 120

Format `wids-security client threshold-value-probe {1-99999}`

Mode Wireless Config

Parameter	*Description*
1–99999	The range of the threshold value.

no wids-security client threshold-value-probe

Use this command to set the threshold value for probe messages to the default.

Format `no wids-security client threshold-value-probe`

Mode Wireless Config

wids-security client threshold-interval-probe

Use this command to configure the threshold interval for counting the probe messages.

Default 60

Format `wids-security client threshold-interval-probe {1-3600}`

Mode Wireless Config

Parameter	*Description*
1–3600	The range of the threshold value.

no wids-security client threshold-interval-probe

Use this command to set the threshold value for the probe interval to its default.

Format `no wids-security client threshold-interval-probe`

Mode Wireless Config

wids-security client threshold-auth-failure

Use this command to configure the number of 802.1X authentication failures that triggers the client to be reported as rogue.

Default 5

Format `wids-security client threshold-auth-failure {1-99999}`

Mode Wireless Config

Parameter	*Description*
1–99999	The range of the threshold value.

no wids-security client threshold-auth-failure

Use this command to set the threshold value for authentication failures to its default.

Format `no wids-security client threshold-auth-failure`

Mode Wireless Config

wids-security client known-db-location

Use this command to configure the location of the Known-Client database for detected clients.

Default Local

Format `wids-security client known-db-location {local | radius-server}`

Mode Wireless Config

Parameter	*Description*
local	Database defined locally.
radius-server	Database defined on a radius-server.

no wids-security client known-db-location

Use this command to set the location of the Known-Client database for detected clients to the default.

Format `no wids-security client known-db-location`

Mode Wireless Config

wids-security client known-db-radius-server-name

Use this command to configure the radius-server name of the Known-Client database for detected clients.

Default Default-RADIUS-Server

Format `wids-security client known-db-radius-server-name name`

Mode Wireless Config

Parameter	*Description*
name	An alphanumeric string up to 32 characters in length.

no wids-security client known-db-radius-server-name

Use this command to set the Known-Client database radius-server name for detected clients to the default.

Format `no wids-security client known-db-radius-server-name`

Mode Wireless Config

detected-client ack-rogue

Use this command to change the client status from Rogue to Known or Authenticated for the specified client MAC address. If no client is specified, the command changes the client status for all of the clients.

Format `detected-client [macaddr] ack-rogue`

Mode Wireless Config

Parameter	*Description*
macaddr	The Ethernet address of the client.

clear wireless detected-client list

Use this command to delete the client entry for the specified MAC address or all the entries present in the database. If the client is authenticated, then this command has no effect.

Format `clear wireless [macaddr] detected-client`

Mode Privileged EXEC

Parameter	*Description*
macaddr	The Ethernet address of the client.

Example: The following shows an example of the command.

```
clear wireless detected-client list
Are you sure you want to clear all the wireless detected clients? (y/n) y
Wireless detected-client list cleared.
```

wireless detected-client roam-history-purge

Use this command to clear the roaming history maintained for a specific MAC address or all the clients present in the detected client database.

Format `wireless detected-client [macaddr] roam-history-purge`

Mode Privileged EXEC

Example: The following shows an example of the command.

```
wireless detected-client roam-history-purge
Are you sure you want to purge the roam history for all of the wireless detected clients? (y/n) y
Roam history purged for all detected-clients.
```

wireless detected-client preauth-history-purge

Use this command to clear the pre-authentication history maintained for the specified MAC address or all the clients present in the detected client database.

Format `wireless detected-client [macaddr] preauth-history-purge`

Mode Privileged EXEC

Example: The following shows an example of the command.

```
wireless detected-client preauth-history-purge
Are you sure you want to purge the pre-auth history for all of the wireless detected clients? (y/n) y
Pre-auth history purged for all detected-clients.
```

show wireless client detected-client pre-auth-history

Use this command to display the pre-authentication events that have occurred for the specified client or for all the clients present in the detected client database. A history of up to ten pre-authentications is displayed, as only a maximum of ten pre-authentications are maintained for each client.

Format `show wireless client [macaddr] detected-client pre-auth-history`

Mode Privileged EXEC

Field	*Description*
Mac Address	The Ethernet address of the client.
AP Mac Address (Radio)	The Ethernet address of the Access Point with which the client is pre-authenticated. (Radio interface number.)

Field	*Description*
Radio	The radio interface on the AP.
VAP Mac Address	The Ethernet address of the VAP to which client has roamed.
SSID	The RF Noise perceived by the reporting AP for the specified detected client.
Pre-Auth Status	Indicates whether the client is successfully pre-authenticated.
Time Since Event	Time since entry was last updated.

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

```
(Switch) # show wireless client detected-client pre-auth-history
Mac Address          AP MAC Address
------------------------------------------------------------------------------
00:02:BB:00:0A:02 <- 00:22:BB:00:14:00 <- 00:00:91:00:50:00 <- 00:22:BB:00:14:00
                  <- 00:00:91:00:50:00
00:02:BB:00:0A:03 <- 00:22:BB:00:14:00
00:02:BB:00:0A:04 <- 00:22:BB:00:14:00 <- 00:00:91:00:50:00 <- 00:22:BB:00:14:00
                  <- 00:00:91:00:50:00 <- 00:00:87:00:50:10 <- 00:22:BB:00:14:00
                  <- 00:00:91:00:50:00 <- 00:00:87:00:50:10 <- 00:22:BB:00:14:00
                  <- 00:00:91:00:50:00

(Switch) # show wireless client 00:02:BB:00:0A:01 detected-client pre-auth-history
AP Mac Addr(Radio)   VAP MAC Address   SSID                Pre-Auth Time since
                                                         Status   event
------------------------------------------------------------------------------
00:22:BB:00:0A:00(1) 00:22:BB:00:0A:01 Test Network1       Success  0d:00:01:51
00:22:BB:00:14:10(2) 00:22:BB:00:14:12 Test Network3       Failure  0d:00:04:40
00:22:BB:00:0A:00(1) 00:22:BB:00:0A:01 Test Network2       Success  0d:00:04:51
00:22:BB:00:14:10(2) 00:22:BB:00:14:13 Network3            Failure  0d:00:05:40
00:02:BB:00:0A:00(1) 00:02:BB:00:0A:01 Test Network3       Success  0d:00:11:51
00:00:91:00:50:10(2) 00:00:91:00:50:12 Test Network1       Failure  0d:00:14:40
00:00:87:00:50:00(1) 00:00:87:00:50:08 Test Network1       Success  0d:00:14:51
00:00:92:00:50:00(1) 00:00:92:00:50:02 Broadcom Network    Failure  0d:00:15:40
```

show wireless client detected-client roam-history

Use this command to display the roaming history for the specified MAC address or all the clients in the detected client database. A roaming history of up to ten Access Points is displayed, as only the maximum of ten records are maintained for each client. Clients that never authenticated with the managed network do not display in the list.

Format `show wireless client macaddr detected-client roam-history`

Mode Privileged EXEC

Field	*Description*
Mac Address	The Ethernet address of the client.
AP Mac Address (Radio)	The Ethernet address of the Access Point with which the client is pre-authenticated.

Field	*Description*
Radio	The radio interface on the AP.
VAP Mac Address	The Ethernet address of the VAP to which client has roamed.
SSID	The RF Noise perceived by the reporting AP for the specified detected client.
Auth Status	Shows if the client authentication was due to new authentication or roaming.
Time Since Roam	Time since entry was last updated.

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

```
(Switch) # show wireless client detected-client roam-history
Mac Address          AP MAC Address
------------------------------------------------------------------------------
00:02:BB:00:0A:01 :: 00:22:BB:00:14:00 <- 00:00:91:00:50:00 <- 00:22:BB:00:14:00
                  <- 00:00:91:00:50:00 <- 00:00:87:00:50:10 <- 00:22:BB:00:14:00
                  <- 00:00:91:00:50:00 <- 00:00:87:00:50:10 <- 00:22:BB:00:14:00
                  <- 00:00:91:00:50:00
00:02:BB:00:0A:02 <- 00:22:BB:00:14:00 <- 00:00:91:00:50:00 <- 00:22:BB:00:14:00
                  <- 00:00:91:00:50:00
00:02:BB:00:0A:03 <- 00:22:BB:00:14:00

(Switch) # show wireless client 00:02:BB:00:0A:01 detected-client roam-history
AP Mac Addr(Radio)   VAP MAC Address   SSID                Auth    Time since
                                                         Status  Roam
------------------------------------------------------------------------------
00:02:BB:00:0A:00(1) 00:02:BB:00:0A:07 Network8            Roam     0d:00:01:51
00:02:BB:00:0A:00(1) 00:02:BB:00:0A:01 TestNetwork2        New Auth 0d:00:02:40
00:02:92:00:0A:10(2) 00:02:92:00:0A:10 Network1            New Auth 0d:00:02:51
00:02:92:00:0A:10(2) 00:02:92:00:0A:12 TestNetwork3        Roam     0d:00:14:40
```

show wireless client detected-client rogue-classification

Use this command to display the WIDS rogue classification test results for a particular client MAC address.

Format `show wireless client macaddr detected-client rogue-classification`

Mode Privileged EXEC

Field	*Description*
macaddr	The client MAC address.
Test ID	Test identifier (WIDSCLNTROGUEnn).
Detect	Indicates whether this test detected the condition that it is designed to detect. Valid values are **no detection** or **Condition Detected**.
MAC Addr (radio)	The Managed AP MAC address and (radio number) that last reported detecting this condition.
Config	Indicates whether this test is configured to report rogues. Valid values are **Enable** or **Disable**.
Result	Indicates whether this test reported the device as rogue. Valid values are **Rogue** or empty string.

Field	*Description*
1st Report	Time stamp indicating how long ago this test first detected the condition.
Last Report	Time stamp indicating how long ago this test last detected the condition.

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

```
(Switch) # show wireless client 00:02:BB:00:14:02 detected-client rogue-classification
WIDSCLNTROGUE1.............................. Client not in Known Client Database
WIDSCLNTROGUE2.............................. Client exceeds configured rate
                                             for auth msgs
WIDSCLNTROGUE3.............................. Client exceeds configured rate
                                             for probe msgs
WIDSCLNTROGUE4.............................. Client exceeds configured rate
                                             for de-auth msgs
WIDSCLNTROGUE5.............................. Client exceeds max failing
                                             authentications
WIDSCLNTROGUE6.............................. Known client authenticated with
                                             unknown AP
```

show wireless client detected-client status

Use this command to display status information for detected clients. If you do not enter a parameter, the command displays summary status for all detected clients in the database. if you enter a client MAC address, the command displays detailed status for that detected client.

Format `show wireless client macaddr detected-client status`

Mode Privileged EXEC

Field	*Description*
MAC Address	The Ethernet address of the client.
OUI	The organizationally unique identifier for the wireless client.
Client Status	The detected client status.
Auth Status	Shows whether the client is authenticated or not.
Time Since Last Updated	Time since entry was last updated.
Threat Detection	Shows if the threat detection test is triggered for this client.
Threat Mitigation	Shows if threat mitigation has been done for this client.
Client Name	Shows the name of the client.
Time Since Created	Time since entry was created.
Channel	Channel in which the client is detected.
Auth RSSI	RSSI reported by the managed AP with which the client is authenticated.
Auth Signal	Signal strength reported by the managed AP with which the client is authenticated.
Auth Noise	Noise reported by the managed AP with which the client is authenticated.

Field	*Description*
Probe Req	Number of probe requests during the collection interval.
Probe Collection Interval	The time remaining in the probe collection interval.
Highest Num Probes	The largest number of probes that the switch detected during the collection interval.
Auth Req	The number of 802.11 authentication messages recorded so far during the probe collection interval.
Auth Collection Interval	The amount of time left before the authentication collection interval is done and the switch decides whether the client is a threat.
Highest Num Auth Msgs	The largest number of authentications that the switch detected during the collection interval.
DeAuth Req	The number of 802.11 de-authentication messages recorded so far during the probe collection interval.
DeAuth Collection Interval	The amount of time left before the de-authentication collection interval is done and the switch decides whether the client is a threat.
Highest Num DeAuth Msgs	The largest number of de-authentications that the switch detected during the collection interval.
Num Auth Failures	The number of 802.1X authentication failures detected for this client.
Total Probe Messages	The number of probes detected in the last RF Scan.
Broadcast BSSID Probes	The number of probes to broadcast BSSID in the last RF Scan.
Broadcast SSID Probes	The number of probes to Broadcast SSID in the last RF Scan.
Specific BSSID Probes	The number of probes to Specific BSSID in the last RF Scan.
Specific SSID Probes	The number of probes to Specific SSID in the last RF Scan.
Last Non-Broadcast BSSID	The last non-broadcast BSSID detected in the RF Scan.
Last Non-Broadcast SSID	The last non-broadcast SSID detected in the RF Scan.
Threat Mitigation Sent	The time since the switch sent the last threat mitigation message to this client.

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

```
(Switch) # show wireless client detected-client status
Mac Address         Client Name    Client Status       Age           Create Time
-------------------------------------------------------------------------------
00:02:BB:00:0A:01   TestClient1    Known               0d:00:01:51    0d:00:01:10
00:02:BB:00:14:02   TestClient2    Rogue               0d:00:14:40    0d:00:14:30

(Switch) # show wireless client 00:13:46:C1:78:67 detected-client status
MAC address..................................... 00:13:46:C1:78:67
```

```
OUI..................................... Broadcom
Client Status........................... Authenticated
Auth Status............................. Authenticated
Time Since Last Updated................. 0d:00:00:02
Threat Detection........................ Detected
Threat Mitigation....................... Not Done
Client Name.............................
Time Since Created...................... 0d:02:17:19
Channel................................. 6
Auth RSSI............................... 14
Auth Signal............................. -81
Auth Noise.............................. -89
Probe Req............................... 12
Probe Collection Interval............... 0d:00:00:41
Highest Num Probes...................... 10
Auth Req................................ 0
Auth Collection Interval................ 0d:00:00:41
Highest Num Auth Msgs................... 0
DeAuth Req.............................. 0
DeAuth Collection Interval.............. 0d:00:00:41
Highest Num DeAuth Msgs................. 0
Num Auth Failures....................... 0
Total Probe Msgs........................ 20
Broadcast BSSID Probes.................. 10
Broadcast SSID Probes................... 10
Specific BSSID Probes................... 0
Specific SSID Probes.................... 0
Last Non-Broadcast BSSID................ 00:00:00:00:00:00
Last Non-Broadcast SSID..................
Threat Mitigation Sent.................. 0d:00:00:00
```

show wireless client detected-client triangulation

Use this command to display the signal triangulation status for the specified client entry.

Format `show wireless client macaddr detected-client triangulation`

Mode Privileged EXEC

Field	*Description*
AP Function	Indicates whether the reporting AP is operating in Sentry Mode.
AP Mac Address	The Ethernet address of the AP.
RSSI	The RSSI value of received signal for the client at the reporting AP.
Signal	The RF signal strength perceived by the reporting AP in dBm for the specified detected-client.
Noise	The RF Noise perceived by the reporting AP for the specified detected-client.
Detected Time	Time in seconds since the particular AP detected the signal.

show wireless wids-security client

Use this command to display the configured wireless WIDS security settings for the client.

Format `show wireless wids-security client`

Mode Privileged EXEC

Field	*Description*
Rogue Detected Trap Interval	Interval, in seconds, between transmissions of the SNMP trap that indicates the administrator that rogue APs are present in the RF Scan database. If set to 0, the trap is never sent.
Rogue-Not in Known Client List	If client MAC address is not in the Known Client database, then report the client as Rogue.
Rogue-Exceeds Auth Req	If the client exceeds the configured rate for transmitting 802.11 authentication requests, report the client as Rogue.
Rogue-Exceeds DeAuth Reg	If the client exceeds the configured rate for transmitting 802.11 de-authentication requests, report the client as Rogue.
Rogue-Exceeds Probe Req	If the client exceeds the configured rate for transmitting probe requests, report the client as Rogue.
Rogue-Exceeds Failed Auth	If the client exceeds the maximum number of failing authentications, report the client as Rogue.
Rogue-Auth Unknown AP	If the Known Client is authenticated with an Unknown AP, report the client as Rogue.
Client Threat-Mitigation	Indicates whether Client Threat Mitigation is enabled or not.
De-auth Threshold Interval	The number of seconds for counting the de-authentication messages.
De-auth Threshold Value	The maximum number of de-authentication messages the client can send without being reported as rogue.
Auth Threshold Interval	The number of seconds for counting the authentication messages.
Auth Threshold Value	The maximum number of authentication messages the client can send without being reported as rogue.
Probe Threshold Interval	The number of seconds for counting the probe messages.
Probe Threshold Value	The maximum number of probe messages the client can send without being reported as rogue.
Auth Failure Threshold	The maximum number of authentication failures that triggers the client to be reported as rogue.
Known DB Location	The location of the Known-Client database for detected clients.
Known DB Radius Server Name	The name of the radius-server for the Known-Client database, defined for detected clients.
Known DB Radius Server Status	Indicates whether or not a radius server for the Known-Client database is configured.

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

```
(Switch) # show wireless wids-security client
Rogue detected trap interval..................... 300 seconds
```

```
Rogue-Not in Known Client list.................. Disable
Rogue-Exceeds Auth Req ......................... Enable
Rogue-Exceeds DeAuth Req ....................... Enable
Rogue-Exceeds Probe Req ........................ Enable
Rogue-Exceeds Failed auth ...................... Enable
Rogue-Auth with unknown AP...................... Disable
Client Threat Mitigation........................ Disable
De-auth threshold interval...................... 60 seconds
De-auth threshold value......................... 10
Auth threshold interval......................... 60 seconds
Auth threshold value............................ 10
Probe threshold interval........................ 60 seconds
Probe threshold value........................... 120
Auth failure threshold.......................... 5
Known DB Location............................... Local
Known DB Radius Server Name..................... Default-RADIUS-Server
Known DB Radius Server Status................... Not Configured
```

show wireless wids-security client rogue-test-descriptions

Use this command to display the WIDS Client rogue classification test identifier descriptions.

Format `show wireless wids-security client rogue-test-descriptions`

Mode Privileged EXEC

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

```
(Switch) # show wireless wids-security client rogue-test-descriptions

WIDSCLIENTROGUE01.........Client not listed in the Known Clients database
WIDSCLIENTROGUE02.........Client exceeds configured rate for transmitting 802.11
                          authentication requests
WIDSCLIENTROGUE03.........Client exceeds configured rate for transmitting probe requests
WIDSCLIENTROGUE04.........Client exceeds configured rate for transmitting de-
                          authentication requests
WIDSCLIENTROGUE05.........Client exceeds max num of failing authentications
WIDSCLIENTROGUE06.........Known Client is authenticated with an Unknown AP
```

Provisioning and Mutual Authentication Commands

This section provides configuration, status and action commands for the provisioning and mutual authentication of peer switches and access points.

switch-provisioning

Use this command to enable switch provisioning.

Default	`enable`
Format	`switch-provisioning`
Mode	Wireless Config

no switch-provisioning

Use the no version of the command to disable switch provisioning.

Format	`no switch-provisioning`
Mode	Wireless Config

agetime ap-provisioning-db

This command configures AP provisioning database entry age times for the wireless switch. A time value of 0 indicates entries in the database will not age and must be manually deleted by an administrator.

Default	`72 hours`
Format	`agetime ap-provisioning-db {0-240}`
Mode	Wireless Config

no agetime ap-provisioning-db

The `no` version of this command returns the configured age time to the default.

Format	`no agetime ap-provisioning-db`
Mode	Wireless Config

mutual-authentication-mode

This command enables the mutual authentication mode for the entire network (or cluster). This command causes configuration to be updated and saved on all switches in the cluster. Switches and APs in the cluster get X.509 certificates to use them in mutual authentication.

Default	`Disable`
Format	`mutual-authentication-mode`
Mode	Wireless Config

no mutual-authentication-mode

The `no` version of this command disables the mutual authentication mode for the entire network (or cluster). This command causes configuration to be updated and saved on all switches in the cluster.

Format	`no mutual-authentication-mode`
Mode	Wireless Config

Example: The following shows an example of the command.

```
(Switch wireless) #mutual-authentication-mode
Enabling Mutual Authentication Mode might result in network traffic disruption. Are you sure you
want to continue? (y/n) y
```

re-provisioning-unmanaged

The command enables re-provisioning of APs when in unmanaged mode. This configuration information is sent to all the switches in the cluster and results in saving of configuration in all switches in the network. This parameter is only applicable if mutual authentication is enabled.

Default	`Enable`
Format	`re-provisioning-unmanaged`
Mode	Wireless Config

no re-provisioning-unmanaged

The `no` version of the command disables re-provisioning for APs in the network when in unmanaged mode.

Format	`no re-provisioning-unmanaged`
Mode	Wireless Config

Example: The following shows an example of the command.

```
(Switch wireless) #re-provisioning-unmanaged
This configuration will be sent to all switches in cluster. Are you sure you want to continue? (y/n) y
```

wireless ap provision switch

This command configures the new primary and the backup switch to be used to for AP when provisioned.

Default `0.0.0.0 - Default`

Format `wireless ap provision macaddr switch {backup | primary} ipaddr`

Mode Privileged EXEC

Field	*Description*
macaddr	MAC address of the AP to be provisioned.
ipaddr	IP address of the primary or the backup switch the AP to be provisioned.

wireless ap provision profile

This command configures the new AP profile to be used to configure this AP when provisioned.

Default `1 - Default`

Format `wireless ap provision macaddr profile {1-16}`

Mode Privileged EXEC

Field	*Description*
macaddr	MAC address of the AP to be provisioned.
profileID	Profile ID to be used when provisioning the AP.

no wireless ap provision profile

The no version of this command sets the provisioning profile ID for the AP to the default value.

Format `no wireless ap provision macaddr profile`

Mode Privileged EXEC

wireless ap provision start

This command initiates provisioning of the specified MAC address or for all the entries present in the AP Provisioning database.

Format `wireless ap provision start`

Mode Privileged EXEC

Field	*Description*
macaddr	MAC address of the AP to be provisioned.

Example: The following shows an example of the command.

```
(Switch) #wireless ap provision start
Are you sure you want to provision all the APs present in the AP provisioning database? (y/n) y
Provisioning of APs present in the database has been initiated.
```

wireless cluster exchange-certificate

This command initiates triggers exchange of X.509 certificates on the switches and APs. This command can be triggered only when network mutual authentication is enabled.

Format `wireless cluster exchange-certificate`

Mode Privileged EXEC

Example: The following shows an example of the command.

```
Switch) #wireless cluster exchange-certificate
Are you sure you want to trigger exchange of X.509 certificates in the cluster? (y/n) y
X.509 certificates exchange has been triggered.
```

clear wireless ap provisioning

This command deletes the entry for the specified mac address or all the entries present in the database. If the AP is *managed* then this command has no effect.

Format `clear wireless ap provisioning [macaddr]`

Mode Privileged EXEC

Example: The following shows an example of the command.

```
(Switch) #clear wireless ap provisioning
Are you sure you want to clear all unmanaged AP provisioning entries? (y/n) y
All unmanaged AP provisioning entries cleared.
```

wireless certificate-generate

This command initiates regeneration of X.509 certificate and RSA key on the wireless switch.

Format `wireless certificate-generate`

Mode Privileged EXEC

Example: The following shows an example of the command.

```
(Switch) #wireless certificate-regenerate
```

show wireless ap provisioning status

This command displays status information for entries in ap provisioning database. If no parameter is entered, the command displays summary status for all entries in the ap provisioning in the database. If a client mac address is entered, detailed status for that entry is displayed.

Format `show wireless ap provisioning [macaddr] status`

Mode Privileged EXEC

Field	*Description*
macaddr	The Ethernet address of the client.
IP Address	IP Address of the AP.
Primary Switch	IP Address of the primary provisioned switch as reported by the AP.
Backup Switch	IP Address of the backup provisioned switch as reported by the AP.
Mutual Authentication Mode	Mutual Authentication mode currently configured on the AP.
Unmanaged AP Re-provisioning Mode	Re-provisioning mode currently configured on the AP.
New Primary Switch	IP Address of the primary switch with switch administrator wants to provision the AP.
New Backup Switch	IP Address of the backup switch with switch administrator wants to provision the AP.
New Profile ID	Profile ID to be configured in the local Valid AP database of new primary and backup switches.
AP Provisioning Status	Status of the most recently issued AP provisioning command.
AP Certificate and Profile Transmit Status	Status of the most last AP profile and certificate distribution to the primary and backup switches.
Time Since Last Update	Time since any information has been received from this AP.

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

```
(Switch) # show wireless ap provisioning status
MAC Address        Primary         Backup          Provisioning  Time Since
                   Switch IP       Switch IP       Status         Last Update
------------------ --------------- --------------- -------------- ------------
```

```
 00:02:BB:00:0A:01 192.168.31.22   192.168.31.21   Not Started    0d:00:01:51
 00:02:BB:00:14:02 192.168.37.23   192.168.33.22   Success        0d:00:14:30

(Switch) # show wireless ap provisioning 00:02:BB:00:0A:01 status
MAC Address..................................... 00:02:BB:00:0A:01
IP Address...................................... 192.168.31.101
Primary Switch.................................. 192.168.31.22
Backup Switch................................... 192.168.31.21
Mutual Authentication Mode...................... Enabled
Unmanaged AP Re-provisioning Mode............... Disabled
New Primary Switch.............................. 192.168.37.22
New Backup Switch............................... 192.168.37.21
New Profile ID.................................. 2
AP Provisioning Status.......................... Success
AP Profile and Certificate Tx. Status.......... Success
Time Since Last Update.......................... 0d:00:02:00
```

Wireless Distribution System-Managed AP Commands

The Wireless Distribution System (WDS)-Managed AP feature allows you to add managed APs to the cluster using over-the-air WDS links through other managed APs. This capability is critical in providing a seamless experience for roaming clients and for managing multiple wireless networks. It can also simplify the network infrastructure by reducing the amount of cabling required. With WDS, APs may be located outdoors where wired connection to the data network is unavailable, or in remote buildings that are not connected to the main campus with a wired network.

The WDS AP group consists of the following managed APs:

- Root AP — Acts as a bridge or repeater on the wireless medium and communicates with the switch via the wired link
- Satellite AP — Communicates with the switch via a WDS link to the Root AP

wds-group (WDS Group Config Mode)

This command adds a new WDS-managed AP group (if not already present) and enters the WDS-managed AP group configuration mode. In this mode, you can modify the WDS-managed AP group's configuration parameters.

Default By default no groups are defined

Format `wds-group {1–8}`

Mode Wireless Config Mode

Parameter	*Description*
1–8	Integer ID for the WDS managed AP group.

no wds-group

The no version of this command deletes a configured WDS managed AP group.

Format `no wds-group {1–8}`

Mode Wireless Config Mode

group-name

This command configures the name for the WDS managed AP group. The default WDS group name for each group is *WDS-AP-Group-* followed by the unique group ID.

Default WDS-AP-Group-*network-id*

Format `group-name name`

Mode WDS AP Group Config Mode

Parameter	*Description*
name	Descriptive name of WDS AP Group, which must be between 1–32 alphanumeric characters.

spanning-tree-mode

This command configures the spanning tree mode for the WDS managed AP group. The default WDS group spanning tree mode is disabled.

Default disabled

Format `spanning-tree-mode [enable | disable]`

Mode WDS AP Group Config Mode

password

This command configures the password used for securing the WPA2-Personal security on the WDS link. The default WDS group password is WDS-AP-Group-*n*, where *n* is the group ID.

Default WDS-AP-Group-*n*

Format `password` *passwd*

Mode WDS AP Group Config Mode

Parameter	*Description*
passwd	ASCII 8–63 characters

ap *macaddr*

This command adds an AP to the WDS managed AP Group.

Format `ap macaddr [spanning-tree priority value]`

Mode WDS Group Config Mode

Default spanning tree priority 36864

Parameter	*Description*
macaddr	MAC address of the AP
value	Spanning tree priority for the AP. Range: 0–61440.

wds-ap-link

This command configures a link between the APs of the WDS Managed AP group and, optionally, sets the spanning tree path cost of the link.

Format `wds-ap-link srcap macaddr radio {1–2} dstap macaddr radio {1–2} [spanning-tree pathcost {0–255}]`

Mode WDS Group Config Mode

Default spanning tree path cost is 40

Parameter	*Description*
srcap *macaddr*	MAC address of the AP that is the source of the WDS link.
dstap *macaddr*	MAC address of the AP that is the destination of the WDS link.
radio {1–2}	Specifies the radio on the destination and source AP to use for the link.
spanning-tree pathcost	Sets the STP path cost of the WDS link to the specified value. Range: 0–255.

show wireless wds-group

This command displays the summary of WDS managed AP group configuration parameters.

Format `show wireless wds-group [wds-group-id]`

Mode Privileged EXEC

Example: The following example shows the output of the `show wireless wds-group` command when no group is specified.

```
(Routing) #show wireless wds-group

Group ID  Group Name                       Spanning-tree  Last Password
Status         change Status
--------  -------------------------------- -------------- ---------------
1         WDS-AP-Group-1                Disable         In Progress
2         WDS-AP-Group-2                Enable          Not Started
```

Example: The following example shows the output of the `show wireless wds-group` command when group 2 is specified.

```
(Routing) #show wireless wds-group 2
WDS Managed AP Group ID..................... 2
Group Name.................................. WDS-AP-Group-2
Spanning Tree Status........................ Disabled
Last password change status................. Not Started
Number of Configured APs.................... 0
Number of Connnected APs.................... 0
Number of Root APs.......................... 0
```

show wireless wds-group ap

This command displays the summary of WDS managed group's Access Points that are part of that group.

Format `show wireless wds-group [{1—8}] ap`

Mode Privileged EXEC

Example: The following example shows the output of the `show wireless wds-group ap` command when group 1 is specified.

```
(Routing) #show wireless wds-group 1 ap

WDS Managed AP Group ID..................... 1

AP MAC Address         STP Priority
-----------------      ------------
11:11:11:11:11:11       34
22:22:22:22:22:22       45
33:33:33:33:33:33       23
44:44:44:44:44:44       32
```

show wireless wds-group link

This command displays the summary of WDS managed group's links configured in that group.

Format `show wireless wds-group [{1—8}] link`

Mode Privileged EXEC

Example: The following example shows the output of the `show wireless wds-group link` command when group 1 is specified.

```
(Routing) #show wireless wds-group 1 link
Source AP MAC      Source  Destination AP     Destination   Path cost
Radio   MAC                Radio
=================  ======  =================  ============  =========
11:12:11:11:13:12    1     11:12:11:11:13:12       1          100
12:12:11:11:13:12    1     11:14:11:11:13:12       2          255
13:12:11:11:13:12    1     11:15:11:11:13:12       1          255
```

show wireless wds-group status

This command displays status information for WDS AP groups that have been configured. If no parameter is entered, the command displays summary status for all entries in the WDS AP group status database. If the WDS Group ID is entered, detailed status for that group is displayed.

Format `show wireless wds-group [{1–8}] status`

Mode Privileged EXEC

Field	*Description*
Group Id	The WDS AP Group Id.
Configured AP Count	Number of APs configured by the Administrator in this WDS AP Group.
Connected AP Count	Number of APs managed by the switch that are member of this WDS AP Group.
Connected Root AP Count	Number of Root APs managed by the switch that are member of this WDS AP Group.
Connected Satellite AP Count	Number of Satellite APs managed by the switch that are member of this WDS AP Group.
Spanning Tree Root Bridge	MAC Address of the device elected as the Spanning Tree Root Bridge
STP Root Device Type	The type of device elected as the Spanning Tree Root bridge
Configured WDS Link Count	Number of configured bidirectional links in the WDS AP Group.
Detected WDS Link Count	Number of WDS links detected in the system.
Blocked WDS Link Count	Number of WDS links blocked by the spanning tree protocol.

Example: The following example shows the output of the `show wireless wds-group status` command when no group is specified.

```
(Routing) # show wireless wds-group status

Group  Configured  Conn. Root  Conn. Satellite  Config. WDS  Detected WDS
Id     AP Count    AP Count    AP Count         Link Count   Link Count
-----  ----------  ----------  ---------------  -----------  ------------
1      5           1           1                4            4
2      4           3           1                6            6
3      6           3           1                4            4
```

Example: The following example shows the output of the `show wireless wds-group status` command when group 1 is specified.

```
(Routing) # show wireless wds-group 1 status

Group Id..................................... 1
Configured AP Count.......................... 5
Connected AP Count........................... 2
Connected Root AP Count...................... 1
Connected Satellite AP Count................. 1
```

```
Spanning Tree Root Bridge..................... 00:00:72:00:50:00
STP Root Device Type.......................... Root AP
Configured WDS Link Count..................... 4
Detected WDS Links Count...................... 6
Blocking WDS Links Count...................... 2
```

show wireless wds-group ap status

This command displays the status information for a specified AP configured in the specified WDS AP group. When the group ID and MAC address is not specified, the command shows the list of all APs in all groups. When the group ID is specified, but the MAC address is not specified then the command shows all APs in the specified group. When the group ID and MAC address both are specified, the command shows detailed information for the AP.

Format `show wireless wds-group {[1–8] ap | 1–8 ap` *macaddr*`} status`

Mode Privileged EXEC

Field	*Description*
Group Id	The WDS AP Group Id.
AP MAC Address	The MAC Address of the AP.
AP Connection Status	Flag indicating whether the AP is currently being managed by one of the Wireless switches in the cluster.
Satellite Mode	Flag indicating whether the AP is a Satellite AP or a Root AP.
Spanning Tree Root Mode	Flag indicating whether this AP is the root of the spanning tree
Root Path Cost	Spanning Tree Path Cost to the root.
Ethernet Port STP Status	Spanning tree status of the Ethernet port.
Ethernet Port Mode	Mode of the Ethernet port.
Ethernet Port Link State	Link state of the Ethernet port.

Example: The following example shows the output of the `show wireless wds-group ap status` command when no group is specified.

```
(Routing) #show wireless wds-group ap status

Group  AP MAC Address     Connection     Satellite  Ethernet Port
Id                        Status         Mode       STP Status
-----  -----------------  -------------  ---------  ------------
1      00:00:91:00:50:00  Connected      Root       Forwarding
1      00:00:92:00:50:00  Not Connected  Root       Learning
2      00:00:93:00:50:00  Connected      Satellite  Listening
```

Example: The following example shows the output of the `show wireless wds-group ap status` command when group 1 is specified.

```
(Routing)#show wireless wds-group 1 ap status

AP MAC Address     Connection     Satellite  Ethernet Port
```

```
Status         Mode       STP Status
-----------------  -------------  ---------  ------------
00:00:91:00:50:00  Connected      Root       Forwarding
00:00:92:00:50:00  Not Connected  Root       Learning
```

Example: The following example shows the output of the `show wireless wds-group ap status` command when group 2 and the AP MAC address is specified.

```
(Routing) #show wireless wds-group 2 ap
00:00:93:00:50:00 status

Group Id..................................... 2
AP MAC Address............................... 00:00:93:00:50:00
AP Connection Status......................... Connected
Satellite Mode............................... Root
Spanning Tree Root Mode...................... STP Root
Root Path Cost............................... 20
Ethernet Port STP Status..................... Forwarding
Ethernet Port Mode........................... Enabled
Ethernet Port Link State..................... Up
```

show wireless wds-group link status

This command displays status information for WDS AP links established in the wireless network. If no parameter is entered, the command displays summary status for all entries in the WDS link status database. If the WDS Group ID is specified, detailed status for that group is displayed.

Format `show wireless wds-group [{1–8}] link status`

Mode Privileged EXEC

Field	*Description*
Group Id	The WDS AP Group Id.
Source MAC Address	The MAC Address of one end-point of the WDS link.
Source Radio	The Radio Number of the WDS Link End-Point on the Source AP.
Destination MAC Address	The MAC Address of other end-point of the WDS link.
Destination Radio	The Radio Number of the WDS Link End-Point on the Destination AP.
Source End-point Detected	The Flag indicating whether AP specified by the Destination MAC detected the AP specified by the source MAC.
Destination End-point Detected	The Flag indicating whether AP specified by the Source MAC detected the AP specified by the Destination MAC.
Aggregation Mode	When parallel links are defined between two APs, this parameter indicates whether this link is part of the aggregation link pair.
Source Spanning Tree State	The Spanning Tree State of the link on the source AP.
Destination Spanning Tree State	The Spanning Tree State of the link on the destination AP.

Example: The following example shows the output of the `show wireless wds-group link status` command when no group is specified.

```
(Routing) #show wireless wds-group link status

Group ID Source MAC        Source Dest MAC          Dest   Source     Dest
Radio                    Radio  Detected   Detected
-------- ----------------- ------ ---------------- -----  ---------  ---------
1        00:00:91:00:50:00 1      00:00:92:00:50:00 1      Yes        Yes
1        00:00:93:00:50:00 1      00:00:94:00:50:00 1      No         Yes
2        00:00:95:00:50:00 1      00:00:96:00:50:00 2      Yes        No
```

Example: The following example shows the output of the `show wireless wds-group link status` command when group 1 is specified.

```
(Routing) #show wireless wds-group 1 link status

WDS Group ID.................................. 1
WDS Group Name................................ WDS-Group-1

Source MAC Address............................ 00:00:91:00:50:00
Source Radio Index............................ 1
Destination MAC Address....................... 00:00:92:00:50:00
Destination Radio Index....................... 1
Source End Point Detected..................... Yes
Destination End Point Detected................ Yes
Aggregation Mode.............................. Aggregated
Source Spanning Tree State.................... Learning
Destination Spanning Tree State............... Forwarding

Source MAC Address............................ 00:00:93:00:50:00
Source Radio Index............................ 1
Destination MAC Address....................... 00:00:94:00:50:00
Destination Radio Index....................... 1
Source End Point Detected..................... Yes
Destination End Point Detected................ No
Aggregation Mode.............................. Aggregated
Source Spanning Tree State.................... Learning
Destination Spanning Tree State............... Disabled
```

show wireless wds-group link statistics

This command displays, for the specified WDS Group ID, the statistics information for WDS AP links established in the wireless network.

Format `show wireless wds-group {1–8} link statistics`

Mode Privileged EXEC

Field	*Description*
Group Id	The WDS AP Group Id.
Source MAC Address	The MAC Address of one end-point of the WDS link.
Source Radio	The Radio Number of the WDS Link End-Point on the Source AP.
Destination MAC Address	The MAC Address of other end-point of the WDS link.

Field	*Description*
Destination Radio	The Radio Number of the WDS Link End-Point on the Destination AP.
Source AP Packets Sent	The number of packets transmitted by the Source AP on the WDS link.
Source AP Bytes Sent	The number of bytes transmitted by the source AP on the link.
Source AP Packets Received	The number of packets received by the Source AP on the WDS link.
Source AP Bytes Received	The number of bytes received by the Source AP on the WDS link.
Destination AP Packets Sent	The number of packets transmitted by the Destination AP on the WDS link.
Destination AP Bytes Sent	The number of bytes transmitted by the Destination AP on the WDS link.
Destination AP Packets Received	The number of packets received by the Destination AP on the WDS link.
Destination AP Bytes Received	The number of bytes received by the Destination AP on the WDS link.

Example: The following example shows the output of the `show wireless wds-group link statistics` command when group 1 is specified.

```
(Routing) #show wireless wds-group 1 link statistics

WDS Group ID.................................. 1
WDS Group Name................................ WDS-Group-1

Source MAC Address............................ 00:00:91:00:50:00
Source Radio Index............................ 1
Destination MAC Address....................... 00:00:92:00:50:00
Destination Radio Index....................... 1
Source AP Packets Sent........................ 100
Source AP Bytes Sent.......................... 1000
Source AP Packets Received.................... 101
Source AP Bytes Received...................... 1010
Destination AP Packets Sent................... 101
Destination AP Bytes Sent..................... 1010
Destination AP Packets Received............... 102
Destination AP Bytes Received................. 1020

Source MAC Address............................ 00:00:93:00:50:00
Source Radio Index............................ 1
Destination MAC Address....................... 00:00:94:00:50:00
Destination Radio Index....................... 1
Source AP Packets Sent........................ 100
Source AP Bytes Sent.......................... 1000
Source AP Packets Received.................... 101
Source AP Bytes Received...................... 1010
Destination AP Packets Sent................... 101
Destination AP Bytes Sent..................... 1010
Destination AP Packets Received............... 102
Destination AP Bytes Received................. 1020
```

wireless wds-group network change-password

This command allows the administrator to set new WDS password for a WDS group.

Format `wireless wds-group {1—8} network change-password`

Mode Privileged EXEC

wireless wds-group network change-password start

This command allows the administrator to initiate WDS group password change to all the peer switches and to all the managed APs in a WDS group.

Format `wireless wds-group {1—8} network change-password start`

Mode Privileged EXEC

Device Location Commands

This section provides configuration, action and status commands for the WLAN device location related information. The Device Location feature can help you physically locate APs and other WLAN devices in different buildings and on multiple floors of a building.

device-location measurement-system

This command configures whether to use English or metric measurement system. When the English measurement system is selected, the device coordinates are configured and displayed in feet. When the metric system is selected the device coordinates are configured and displayed in meters. If the measurement system is changed when some devices are already configured, the device coordinates are converted to the newly selected measurement system.

Default metric

Format `device-location measurement-system {english| metric}`

Mode Wireless Config Mode

device-location rf-scan

This command configures the RF-scan device location mode for the switch. This mode indicates whether the switch computes device location from the RF-Scan reports for the device. When this mode is enabled, the location is stored in the device triangulation table.

Default Enable

Format `device-location rf-scan`

Mode Wireless Config Mode

no device-location rf-scan

This command disables the RF-Scan device location mode configuration for the switch.

Format no device-location rf-scan

Mode Wireless Config Mode

device-location rf-scan interval

This command configures the RF-scan device location interval, in seconds, for the wireless switch. The interval is the number of seconds between the iterations of the triangulation table device location protocol.

Default 60 seconds

Format `device-location rf-scan interval {30-3600}`

Mode Wireless Config Mode

no device-location rf-scan interval

The no version of this command returns the configured RF-scan interval to default.

Format `no device-location rf-scan interval`

Mode Wireless Config Mode

device-location building

This command adds the building number (if not present) and enters the building configuration mode. The building is identified by building number.

Default building – None

Format `device-location building {1–8}`

Mode Wireless Config Mode

Parameter	*Description*
1–8	Building Number
`building-description`	Building Description

no device-location building

The no version of this command deletes the building entry for the specified building number from the database.

Format `no device-location building {1-8}`

Mode Wireless Config Mode

Parameter	*Description*
1–8	Building Number

description (Building)

This command adds a description to the building to make it easier to identify. For example, the *`building-description`* parameter could be “101 Technology Drive.” Include quotation marks if the description includes spaces.

Default Building-*n*, where *n* is the building number (1–8).

Format `description` *`building-description`*

Mode Device Location Building Config Mode

Parameter	*Description*
`building-description`	User-specified description of the building

no description (Building)

This command resets the building description to the default value.

Format `no description`

Mode Device Location Building Config Mode

floor

This command adds the floor number (if not present) for a floor in the building and enters the floor configuration mode. The floor is identified by floor number.

Default floor – None

Format `floor {1–20}`

Mode Device Location Building Config Mode

Parameter	*Description*
1–20	Floor Number

no floor

The no version of this command deletes the floor entry for the specified floor number from the database.

Format `no floor {1–20}`

Mode Device Location Building Config Mode

ap

This command adds the AP mac address in a particular floor and building. Further the corresponding x,y coordinates for the AP are configured. X and Y coordinates are the offsets of the managed AP from some arbitrary 0,0 point on the building floor. If the measurement system is set as metric, the range for the X and the Y coordinates varies from –1000 to 1000 metres, if English then the range varies from –3000 to 3000 feet.

Default None

Format `ap` *`macaddr`* `xy-coordinate {feet | metres}` *`x-coordinate y-coordinate`*

Mode Device Location Floor Config Mode

Parameter	*Description*
macaddr	AP MAC address.
`feet`	The device coordinates are configured in feet.
`metres`	The device coordinates are configured in meters.
`x-coordinate`	X axis offset of the device.
`y-coordinate`	Y axis offset of the device.

Example: The following example shows how to configure an AP with the MAC address 00:00:91:00:50:00 on a floor that is at the 100 × 200 foot coordinate on the floor.

```
(Switch)(Config-building-floor)#ap 00:00:91:00:50:00 xy-coordinate feet 100 200
```

Example: The following example shows how to configure an AP with the MAC address 00:00:91:00:50:00 on a floor that is at the 150 × 100 meter coordinate on the floor.

```
(Switch)(Config-building-floor)#ap 00:00:92:00:50:00 xy-coordinate
metres 150 100
```

no ap

The no version of this command deletes the AP mac address and its corresponding x,y coordinates for the specified floor and building number from the database.

Format no ap *macaddr*

Mode Device location Floor Config Mode

description (Floor)

This command adds a description to the floor.

Default None

Format description *floor-description*

Mode Device Location Floor Config Mode

Parameter	*Description*
floor-description	User-specified description of the floor.

no description (Floor)

This command resets the floor description to the default value.

Format no description

Mode Device Location Floor Config Mode

show wireless device-location

This command displays entries for the Device location Measurement System, RF-Scan and RF-Scan Interval.

Format `show wireless device-location`

Mode Privileged EXEC

Example: The following example shows the output of the `show wireless device-location` command.

```
(Switch) #show wireless device-location

Device Location Measurement System.............Metric
Device Location RF-Scan.....................  Enable
Device Location RF-Scan Interval.............  60
```

show wireless device-location building

This command displays the building entries. If no parameters are entered, a summary for all configured buildings is displayed.

Format `show wireless device-location building [{1–8}]`

Mode Privileged EXEC

Parameter	*Description*
1–8	Building Number

Field	*Description*
Building Number	The building number.
Building Description	The building description of a particular building
Total Floor Count	The floor number associated with the building.
Total AP Count	The floor description of a particular floor.

Example: The following example shows the output of the `show wireless device-locator building` command when no building is specified. This command is executed on the Cluster Controller.

```
(Switch) #show wireless device-location building

Building    Building      Total Floor   Total AP
Number      description   Count         Count
-----------------------------------------------------
1           building-1     6            6
2           building-2     3            3
```

Example: The following example shows the output of the `show wireless device-locator building` command when building 1 is specified.

```
(Switch) #show wireless device-location building 1
Building Number.............. 1
Building Description........... building-1
Total Floor Count.............. 6
Total AP Count................. 6
```

show wireless device-location building floor

This command displays all the floor details of the specified building number. If no building or floor is specified a summary of floor status for all buildings is displayed.

Format `show wireless device-location building [{1–8}] floor [{1–20}]`

Mode Privileged EXEC

Parameter	*Description*
1–8	Building number
1–20	Floor number

Field	*Description*
building –number	The building number.
building-description	The building description of a particular building
floor number	The floor number associated with the building.
floor-description	The floor description of a particular floor.
Total AP Count	The total number of APs within the building.

Example: The following example shows the output of the `show wireless device-location building floor` command when no buildings or floors are specified. This command is executed on the Cluster Controller,

```
(Switch) #show wireless device-location building floor

Building/       Floor
Floor Number    Description    AP Count
-----------------------------------------------
1/1              floor-1       1
1/2              floor-2       1
1/3              floor-3       1
1/4              floor-4       1
1/5              floor-5       1
1/6              floor-6       1
2/1              floor-1       1
2/2              floor-2       1
2/3              floor-3       1
```

Example: The following example shows the output of the `show wireless device-location building floor` command when building 1 and no floors are specified. This command is executed on the Cluster Controller,

```
(Switch) #show wireless device-location building 1 floor
Floor         Floor
Number        Description    AP Count
-----------------------------------------------------
1             floor-1        1
2             floor-2        1
3             floor-3        1
4             floor-4        1
5             floor-5        1
6             floor-6        1
```

Example: The following example shows the output of the `show wireless device-location building floor` command when buildings 1 and floor 1 are specified. This command is executed on the Cluster Controller,

```
(Switch) #show wireless device-location building 1 floor 1
Building Number.............. 1
Building Description........... building-1
Floor Number.................. 1
Floor Description.............. floor-1
Total AP Count................. 1
```

show wireless device-location building floor ap

This command displays all the APs in the specified floor and building. If no parameters are entered, a summary is displayed. You can enter a building number, floor number to display detailed information for a specific building and floor.

Format `show wireless device-location building [{1—8}] floor [{1—20}] ap`

Mode Privileged EXEC

Parameter	*Description*
1–8	Building number
1–20	Floor number

Field	*Description*
building –number	The building number.
floor number	The floor number associated with the building.
AP-MAC	The mac address of the AP in the building.
XY-Coordinate	The xy-coordinate of the particular location.

Example: The following example shows the output of the `show wireless device-location building floor ap` command when no building or floor is specified. This command is executed on the Cluster Controller.

```
(Switch) #show wireless device-location building floor ap
Building/       AP Mac               XY-Coordinate
Floor Number    Address
```

```
-----------------------------------------------------------------
1/1          00:00:91:00:50:00     30, 40
1/2          00:00:92:00:50:00     12, -9
1/3          00:00:93:00:50:00    -100, 100
1/4          00:00:71:00:50:00     100, 100
1/5          00:00:72:00:50:00    -10, 100
1/6          00:00:73:00:50:00    -1, 100
2/1          00:00:74:00:50:00     1,-1
2/2          00:00:75:00:50:00     9,-12
2/3          00:00:76:00:50:00     2, 90
```

Example: The following example shows the output of the `show wireless device-location building floor ap` command when building 1 and no floor is specified. This command is executed on the Cluster Controller.

```
(Switch) #show wireless device-location building 1 floor ap
Floor             AP Mac                XY-Coordinate
Number            Address
-------------------------------------------------------------
1             00:00:91:00:50:00       30, 40
2             00:00:92:00:50:00       12, -9
3             00:00:93:00:50:00      -100, 100
4             00:00:71:00:50:00       100, 100
5             00:00:72:00:50:00      -10, 100
6             00:00:73:00:50:00       - 1, 100
```

Example: The following example shows the output of the `show wireless device-location building floor ap` command when building 1 and floor 1 are specified. This command is executed on the Cluster Controller.

```
(Switch) #show wireless device-location building 1 floor 1 ap
AP Mac                   XY-Coordinate
Address
--------------------------------------
00:00:91:00:50:00         30, 40
```

show wireless device-location triangulation status

This command displays status information for entries in the triangulation table. If no parameter is entered, the command displays summary status for all entries in the triangulation table database. If an AP or a client MAC address is entered, detailed status for that entry is displayed.

Format `show wireless device-location {ap | client} [macaddr] triangulation {status-all | status-located}`

Mode Privileged EXEC

Parameter	*Description*
macaddr	AP/Client MAC address
status-all	Display Triangulation Location status parameters for all device entries in the triangulation table database.
status-located	Display Triangulation Location status parameters for located device entries in the triangulation table database.

Field	*Description*
Device MAC Address	The AP or Client MAC Address whose location is reported.
Device type	The device type, which is either AP or Client.
Location Data	The location of the device whether present or not.
Location Computation Status	Status of the last iteration of location computation algorithm.
Last Successful Computation	Time since the last successful location computation.
Building Number	Building number in which the device is detected.
Floor Number	Floor number in which the device is detected.
Detected X-Coordinate	X axis offset on the device of the building floor
Detected Y-Coordinate	Y axis offset on the device of the building floor

Example: The following example shows the output of the `show wireless device-location triangulation status` command for all entries in the triangulation table database. This command is executed on the Cluster Controller.

```
(Switch) # show wireless device-location ap triangulation status-all
Device MAC        Device   Building/   Detected     Last
Address           Type     Floor       XY           Computation
                           Number      Coordinate   Status
----------------- ------- ----------   ----------- ------------

00:00:91:00:50:00   AP      0/0         0,0         Not Executed
00:00:92:00:50:00   AP      2/2         -100,10     Success
00:00:93:00:50:00   AP      3/1         -111,100    Success
00:00:94:00:50:00   AP      4/1         -1,10       Success
```

Example: The following example shows the output of the `show wireless device-location triangulation status` command for a specific AP. This command is executed on the Cluster Controller.

```
(Switch) # show wireless device-location  ap 00:00:91:00:50:00 triangulation status

Device MAC Address.............................. 00:00:91:00:50:00
Device Type..................................... AP
Location Data................................... Not present
Location Computation Status..................... Not Executed
Last Successful Computation..................... 0d:00:00:05
Building Number................................. 1
Floor Number.................................... 1
Detected X-Coordinate........................... 0
Detected Y-Coordinate........................... 0
```

Example: The following example shows the output of the `show wireless device-location triangulation status` command for all entries in the triangulation table database. This command is executed on the Cluster Controller.

```
(Switch) # show wireless device-location ap triangulation status-located
Device MAC        Device   Building/   Detected    Last
Address           Type     Floor       XY          Computation
                           Number      Coordinate  Status
----------------- ------- ----------   ----------- ------------
00:00:92:00:50:00   AP      2/2          -100,10    Success
00:00:93:00:50:00   AP      3/1          -111,100   Success
00:00:94:00:50:00   AP      4/1          -1,10      Success
```

Example: The following example shows the output of the `show wireless device-location triangulation status` command for all entries in the triangulation table database. This command is executed on the Cluster Controller.

```
(Switch) # show wireless device-location client triangulation status-all
Device MAC        Device   Building/   Detected    Last
Address           Type     Floor       XY          Computation
                           Number      Coordinate  Status
----------------- ------- ----------   ----------- ------------
00:02:BB:00:0A:01   Client  0/0          0/0        Not Executed
00:02:BB:00:0A:02   Client  2/1          -100,1000  Success
00:02:BB:00:0A:03   Client  3/2          -11,11     Success
00:02:BB:00:0A:04   Client  4/2          -14,10     Success
```

Example: The following example shows the output of the `show wireless device-location triangulation status` command for all entries in the triangulation table database. This command is executed on the Cluster Controller.

```
(Switch) # show wireless device-location client 00:02:BB:00:0A:01 triangulation status

Device MAC Address.............................. 00:02:BB:00:0A:01
Device Type..................................... Client
Location Data................................... Not present
Location Computation Status..................... Not Executed
Last Successful Computation..................... 0d:00:00:05
Building Number................................. 1
Floor Number.................................... 2
Detected X-Coordinate........................... 0
Detected Y-Coordinate........................... 0

(Switch) # show wireless device-location client triangulation status-located
```

```
Device MAC        Device   Building/   Detected     Last
Address           Type     Floor       XY           Computation
                           Number      Coordinate   Status
----------------- ------- ----------   ----------- ------------
00:02:BB:00:0A:02   Client  2/1          -100,1000  Success
00:02:BB:00:0A:03   Client  3/2          -11,11     Success
00:02:BB:00:0A:04   Client  4/2          -14,10     Success
```

wireless device-location start-search

This command is used to trigger the location search for an AP or client with the given MAC address. Optionally, you can specify the building number and floor number to search for the target device. If the building number is specified, the wireless system searches for the target devices on all the floors in the building. If the floor number is also specified, then it is searches only in the specified building and floor. If you do not specify the building number and floor number, the target device is searched in all the buildings and floors across the wireless system.

You can also specify to use operational mode radios for searching the target device. If you choose to use operational mode radios in the search, a prompt is displayed to confirm that traffic for existing WLAN clients will be disrupted as operational radios are being used for search.

As soon as you trigger a search, all of the configured parameters along with the number of locator APs are shown and a prompt is displayed to confirm that you want to trigger the device location search with the specified parameters.

If you attempt to trigger a new search while a search is already in progress, the following error message displays: `Location search is already in progress and new search is not initiated`. However, the search parameters are saved.

Format `wireless device-location start-search {ap | client} macaddr [building {1–8}] [floor {1–20}] [use-operational-mode-radios]`

Mode Privileged EXEC

Field	*Description*
macaddr	The mac address of the AP or client to locate.
1–8	Building number in which to search for the target device.
1–20	Floor number on which to search for the target device.

Example: The following example shows the output of the `wireless device-location start-search` command when the client MAC address is specified.

```
(Routing) #wireless device-location start-search client 00:08:A1:7E:58:A3

Device Type:................................. Client
Device MAC Address:.......................... 00:08:A1:7E:58:A3
Building:.................................... All
Floor:....................................... All
Number of Locator APs:....................... 18
```

```
Use Operational Mode Radios:.................. No

Trigger device location search with above parameters? (y/n) y

Device Location Search is triggered.
```

Example: The following example shows the output of the `wireless device-location start-search` command when the AP MAC address and `use-operational-mode-radios` keyword are specified.

```
(Routing) #wireless device-location start-search ap 00:1b:e9:16:2c:40 use-operational-mode-
radios

Device Type:................................. AP
Device MAC Address:.......................... 00:1B:E9:16:2C:40
Building:.................................... All
Floor:....................................... All
Number of Locator APs:....................... 18
Use Operational Mode Radios:................. Yes

Traffic for existing WLAN clients will be disrupted as operational
radios are being used for search.

Trigger device location search with above parameters? (y/n) n

Device Location Search is not triggered.
```

Example: The following example shows the output of the `wireless device-location start-search` command when the client MAC address and building are specified.

```
(Routing) #wireless device-location start-search
client 00:1f:3c:22:cb:57 building 6

Device Type:................................. Client
Device MAC Address:.......................... 00:1F:3C:22:CB:57
Building:.................................... 6
Floor:....................................... All
Number of Locator APs:....................... 9
Use Operational Mode Radios:................. No

Trigger device location search with above parameters? (y/n) n

Device Location Search is not triggered.
```

Example: The following example shows the output of the `wireless device-location start-search` command when the client MAC address, building number, and `use-operational-mode-radios` keyword are specified.

```
(Routing) #wireless device-location start-search client 00:08:A1:7E:58:A3 building 4 use-
operational-mode-radios

Device Type:................................. Client
Device MAC Address:.......................... 00:08:A1:7E:58:A3
Building:.................................... 4
Floor:....................................... All
Number of Locator APs:....................... 5
Use Operational Mode Radios:................. Yes
```

```
Traffic for existing WLAN clients will be disrupted as operational
radios are being used for search.

Trigger device location search with above parameters? (y/n) y

Device Location Search is triggered.
```

Example: The following example shows the output of the `wireless device-location start-search` command when the AP MAC address, building number, and floor number are specified.

```
(Routing) #wireless device-location start-search ap 00:11:22:33:88:40 building 6 floor 18

Device Type:................................... AP
Device MAC Address:............................ 00:11:22:33:88:40
Building:...................................... 6
Floor:......................................... 18
Number of Locator APs:......................... 4
Use Operational Mode Radios:................... No

Trigger device location search with above parameters? (y/n) n

Device Location Search is not triggered.
```

Example: The following example shows the output of the `wireless device-location start-search` command when the AP MAC address, building number, floor number, and `use-operational-mode-radios` keyword are specified.

```
(Routing) #wireless device-location start-search ap  00:1b:e9:16:2c:40 building 2 floor 5  use-
operational-mode-radios

Device Type:................................... AP
Device MAC Address:............................ 00:1B:E9:16:2C:40
Building:...................................... 2
Floor:......................................... 5
Number of Locator APs:......................... 3
Use Operational Mode Radios:................... Yes

Traffic for existing WLAN clients will be disrupted as operational
radios are being used for search.

Trigger device location search with above parameters? (y/n) y

Device Location Search is triggered.
```

show wireless device-location global-status

This commands reports the parameters that are actually used in the previous run of the location search procedure. It also reports the global status of the last invocation of the On-Demand Location Procedure.

Format `show wireless device-location global-status`

Mode Privileged EXEC

Field	*Description*
Device Type	Type of the device located.
Device MAC	The MAC Address of the device whose location was requested.
Building	Building number in which to search for the target device was done.
Floor	Floor Number on which the search was done.
Number of Locator APs	Number of managed APs that were used for locating the target device.
Use Operational Mode Radios	Indicates whether the network used only sentry radios to do the search or both sentry and operational mode radios.
Location Procedure Status	Current status of the last invocation of the On-Demand Location Procedure.
Number of Detecting APs	Number of managed APs that detected the device.
Number of buildings with Detected Signal	Number of buildings where managed APs detected the target device.
Number of floors with detected signal	Number of building floors where managed APs detected the target device.
Building with the Highest Detected Signal	Building number in which the target device was detected by a managed AP with the highest RSSI.
Floor with the Highest Detected Signal	Floor number on which the target device was detected by a managed AP with the highest RSSI.

Example: The following examples show the output of the `show wireless device-location global-status` command.

```
(Routing) #show wireless device-location global-status

Device Type:................................ Client
Device MAC Address:......................... 00:1F:3C:CB:11:57
Building:................................... All
Floor:...................................... All
Use Operational Mode Radios:................ No
Location Procedure Status:.................. In Progress
Number of Locator APs:...................... 18
Number of Detecting APs:.................... 0
Number of Buildings with Detected Signal:..... 0
Number of Floors with Detected Signal:........ 0
Building with the Highest Detected Signal:.... 0
Floor with the Highest Detected Signal:....... 0
```

```
(Routing) #show wireless device-location global-status

Device Type:................................... AP
Device MAC Address:............................ 00:1B:E9:16:2C:40
Building:...................................... 5
Floor:......................................... All
Use Operational Mode Radios:................... Yes
Location Procedure Status:..................... Device located
Number of Locator APs:......................... 14
Number of Detecting APs:....................... 8
Number of Buildings with Detected Signal:...... 1
Number of Floors with Detected Signal:......... 10
Building with the Highest Detected Signal:..... 5
Floor with the Highest Detected Signal:........ 6

(Routing) #show wireless device-location global-status

Device Type:................................... Client
Device MAC Address:............................ 00:08:A1:7E:58:A3
Building:...................................... 7
Floor:......................................... 15
Use Operational Mode Radios:................... Yes
Location Procedure Status:..................... No APs Available for Locating Device
Number of Locator APs:......................... 0
Number of Detecting APs:....................... 0
Number of Buildings with Detected Signal:...... 0
Number of Floors with Detected Signal:......... 0
Building with the Highest Detected Signal:..... 0
Floor with the Highest Detected Signal:........ 0

(Routing) #show wireless device-location global-status

Device Type:................................... Client
Device MAC Address:............................ 00:08:A1:7E:58:A3
Building:...................................... 3
Floor:......................................... 12
Use Operational Mode Radios:................... Yes
Location Procedure Status:..................... Device is not located
Number of Locator APs:......................... 4
Number of Detecting APs:....................... 0
Number of Buildings with Detected Signal:...... 0
Number of Floors with Detected Signal:......... 0
Building with the Highest Detected Signal:..... 0
Floor with the Highest Detected Signal:........ 0
```

show wireless device-location floor-status

This commands reports location information for each floor.

Format `show wireless device-location floor-status [building {1—8}] [floor {1—20}]`

Mode Privileged EXEC

Field	*Description*
1–8	Building number to view the location information.
1–20	Floor number to view the location information.

Field	*Description*
Device Found	Indicates whether the device is found on this floor.
Number of APs	Number of APs located on this floor that detected the device.
Solution Type	Flag indicating whether the a probability map is a circle around the managed AP, or the solution is an X,Y coordinate.
X-axis Coordinate	X-axis offset. The parameter is applicable to the Circle and Point solution.
Y-axis Coordinate	Y-axis offset. The parameter is applicable to the Circle and Point solution.
Circle Radius	For the Circle solution this parameter represents the radius from the X,Y coordinate where the device is most likely to be located. For the Point solution this value is not applicable and is set to 0.
Sigma	The standard deviation for the location. The parameter is applicable to Circle and Point solutions. For the Circle solution the Sigma represents the offset from *Circle Radius*. For the Point solution the sigma represents the radius from the X,Y coordinate.

Example: The following examples show the output of the `show wireless device-location floor-status` command when no optional parameters are specified.

```
(Routing) #show wireless device-location floor-status

Building/ Device    Number of Solution    (X,Y)       Circle Sigma
Floor     Found     APs       Type        (Meters)    Radius (Meters)
--------- --------- --------- ----------- ----------- ------ --------
2/3       Not Found 0         No Solution (0,0)       0      0
2/4       Found     2         Point       (126,-161)  0      5
2/5       Found     6         Circle      (103,56)    7      2
4/6       Found     3         Point       (25,80)     0      1
6/7       Found     1         Circle      (-45,25)    20     5
6/18      Found     9         Point       (-51,-123)  0      2
```

Example: The following examples show the output of the `show wireless device-location floor-status` command when the building number is specified.

```
(Routing) #show wireless device-location floor-status building 6

Building/ Device    Number of Solution    (X,Y)       Circle Sigma
Floor     Found     APs       Type        (Meters)    Radius (Meters)
```

```
--------- ------    --------- ----------- ----------- ------ --------
6/7       Found     1         Circle      (-45,25)    20     5
6/18      Found     9         Point       (-51,-123)  0      2
```

Example: The following examples show the output of the `show wireless device-location floor-status` command when the building number and floor number are specified.

```
(Routing) #show wireless device-location floor-status
building 2 floor 4

Device Found.................................. Found
Number of APs................................. 2
Solution Type................................. Point Solution
X-axis Coordinate............................. 126 Meters
Y-axis Coordinate............................. -161 Meters
Circle Radius................................. 0 Meters
Sigma......................................... 5 Meters
```

Section 9: Quality of Service Commands

This chapter describes the Quality of Service (QoS) commands available in the DWS-4000 CLI.

The QoS Commands chapter contains the following sections:

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

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

Class of Service Commands

This section describes the commands you use to configure and view Class of Service (CoS) settings for the switch. The commands in this section allow you to control the priority and transmission rate of traffic.

Note: Commands you issue in the Interface Config mode only affect a single interface. Commands you issue in the Global Config mode affect all interfaces.

classofservice dot1p-mapping

This command maps an 802.1p priority to an internal traffic class. The *userpriority* values can range from 0–7. The *trafficclass* values range from 0–6, although the actual number of available traffic classes depends on the platform. For more information about 802.1p priority, see "Voice VLAN Commands" on page 250.

Format `classofservice dot1p-mapping` *`userpriority trafficclass`*

Modes
- Global Config
- Interface Config

no classofservice dot1p-mapping

This command maps each 802.1p priority to its default internal traffic class value.

Format `no classofservice dot1p-mapping`

Modes
- Global Config
- Interface Config

classofservice ip-dscp-mapping

This command maps an IP DSCP value to an internal traffic class. The *ipdscp* value is specified as either an integer from 0 to 63, or symbolically through one of the following keywords: `af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, ef`.

The *trafficclass* values can range from 0–6, although the actual number of available traffic classes depends on the platform.

Format `classofservice ip-dscp-mapping` *`ipdscp trafficclass`*

Mode Global Config

no classofservice ip-dscp-mapping

This command maps each IP DSCP value to its default internal traffic class value.

Format `no classofservice ip-dscp-mapping`

Mode Global Config

classofservice trust

This command sets the class of service trust mode of an interface or range of interfaces. You can set the mode to trust one of the Dot1p (802.1p), IP DSCP, or IP Precedence packet markings. You can also set the interface mode to untrusted. If you configure an interface to use Dot1p, the mode does not appear in the output of the `show running config` command because Dot1p is the default.

Note: The `classofservice trust dot1p` command will not be supported in future releases of the software because Dot1p is the default value. Use the `no classofservice trust` command to set the mode to the default value.

Default dot1p

Format `classofservice trust {dot1p | ip-dscp | ip-precedence | untrusted}`

Modes
- Global Config
- Interface Config

no classofservice trust

This command sets the interface mode to the default value.

Format `no classofservice trust`

Modes
- Global Config
- Interface Config

cos-queue min-bandwidth

This command specifies the minimum transmission bandwidth guarantee for each interface queue on an interface, a range of interfaces, or all interfaces. The total number of queues supported per interface is platform specific. A value from 0–100 (percentage of link rate) must be specified for each supported queue, with 0 indicating no guaranteed minimum bandwidth. The sum of all values entered must not exceed 100.

Format `cos-queue min-bandwidth` *`bw-0 bw-1 … bw-n`*

Modes
- Global Config
- Interface Config

no cos-queue min-bandwidth

This command restores the default for each queue's minimum bandwidth value.

Format `no cos-queue min-bandwidth`

Modes
- Global Config
- Interface Config

cos-queue random-detect

This command activates weighted random early discard (WRED) for each specified queue on the interface. Specific WRED parameters are configured using the `random-detect queue-parms` and the `random-detect exponential-weighting-constant` commands.

Format `cos-queue random-detect queue-id-1 [queue-id-2 … queue-id-n]`

Modes
- Global Config
- Interface Config

When specified in Interface Config' mode, this command affects a single interface only, whereas in Global Config mode, it applies to all interfaces.

At least one, but no more than *n*, queue-id values are specified with this command. Duplicate queue-id values are ignored. Each queue-id value ranges from 0 to (*n*–1), where n is the total number of queues supported per interface. The number *n* is platform dependent and corresponds to the number of supported queues (traffic classes).

no cos-queue random-detect

Use this command to disable WRED, thereby restoring the default tail drop operation for the specified queues on the interface.

Format `no cos-queue random-detect queue-id-1 [queue-id-2 … queue-id-n]`

Modes
- Global Config
- Interface Config

cos-queue strict

This command activates the strict priority scheduler mode for each specified queue for an interface queue on an interface, a range of interfaces, or all interfaces.

Format `cos-queue strict queue-id-1 [queue-id-2 … queue-id-n]`

Modes
- Global Config
- Interface Config

no cos-queue strict

This command restores the default weighted scheduler mode for each specified queue.

Format `no cos-queue strict queue-id-1 [queue-id-2 … queue-id-n]`

Modes
- Global Config
- Interface Config

random-detect

This command is used to enable WRED for the interface as a whole, and is only available when per-queue WRED activation control is not supported by the device Specific WRED parameters are configured using the `random-detect queue-parms` and the `random-detect exponential-weighting-constant` commands.

Format `random-detect`

Modes
- Global Config
- Interface Config

When specified in Interface Config mode, this command affects a single interface only, whereas in Global Config mode, it applies to all interfaces. The Interface Config mode command is only available on platforms that support independent per-port class of service queue configuration.

no random-detect

Use this command to disable WRED, thereby restoring the default tail drop operation for all queues on the interface.

Format `no random-detect`

Modes
- Global Config
- Interface Config

random-detect exponential weighting-constant

This command is used to configure the WRED decay exponent for a CoS queue interface.

Format `random-detect exponential-weighting-constant` *`1-TBD`*

Modes
- Interface Config

random-detect queue-parms

This command is used to configure WRED parameters for each drop precedence level supported by a queue. It is used only when per-COS queue configuration is enabled (using the `cos-queue random-detect` command).

Format `random-detect queue-parms` *`queue-id-1`* [*`queue-id-2 … queue-id-n`*] `min-thresh` *`thresh-prec-1 … thresh-prec-n`* `max-thresh` *`thresh-prec-1 … thresh-prec-n`* `drop-probability` *`prob-prec-1 … prob-prec-n`*

Modes
- Global Config
- Interface Config

Each parameter is specified for each possible drop precedence (*color* of TCP traffic). The last precedence applies to all non-TCP traffic. For example, in a 3-color system, four of each parameter specified: green TCP, yellow TCP, red TCP, and non-TCP, respectively.

Term	*Definition*
min-thresh	The minimum threshold the queue depth (as a percentage) where WRED starts marking and dropping traffic.
max-thresh	The maximum threshold is the queue depth (as a percentage) above which WRED marks / drops all traffic.
drop-probability	The percentage probability that WRED will mark/drop a packet, when the queue depth is at the maximum threshold. (The drop probability increases linearly from 0 just before the minimum threshold, to this value at the maximum threshold, then goes to 100% for larger queue depths).

no random-detect queue-parms

Use this command to set the WRED configuration back to the default.

Format `no random-detect queue-parms` *queue-id-1* [*queue-id-2 … queue-id-n*]

Modes
- Global Config
- Interface Config

traffic-shape

This command specifies the maximum transmission bandwidth limit for the interface as a whole. You can also specify this value for a range of interfaces or all interfaces. Also known as rate shaping, traffic shaping has the effect of smoothing temporary traffic bursts over time so that the transmitted traffic rate is bounded.

Format `traffic-shape` *bw*

Modes
- Global Config
- Interface Config

no traffic-shape

This command restores the interface shaping rate to the default value.

Format `no traffic-shape`

Modes
- Global Config
- Interface Config

show classofservice dot1p-mapping

This command displays the current Dot1p (802.1p) priority mapping to internal traffic classes for a specific interface. 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 “Voice VLAN Commands” on page 250.

Format `show classofservice dot1p-mapping [slot/port]`

Mode Privileged EXEC

The following information is repeated for each user priority.

Term	*Definition*
User Priority	The 802.1p user priority value.
Traffic Class	The traffic class internal queue identifier to which the user priority value is mapped.

show classofservice ip-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.

Term	*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.

Term	*Definition*
IP DSCP	The IP DSCP value.
Traffic Class	The traffic class internal queue identifier to which the IP DSCP value is mapped.

show classofservice trust

This command displays the current trust mode setting for a specific interface. 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

Term	*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

Term	*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.

Term	*Definition*
Interface	The slot/port of the interface. If displaying the global configuration, this output line is replaced with a Global Config indication.
Interface Shaping Rate	The maximum transmission bandwidth limit for the interface as a whole. It is independent of any per-queue maximum bandwidth value(s) in effect for the interface. This is a configured value.

show interfaces random-detect

This command displays the global WRED settings for each CoS queue. If you specify the slot/port, the command displays the WRED settings for each CoS queue on the specified interface.

Format `show interfaces random-detect [slot/port]`

Mode Privileged EXEC

Term	*Definition*
Queue ID	An interface supports n queues numbered 0 to (n-1). The specific n value is platform dependent.
WRED Minimum Threshold	The configured minimum threshold the queue depth (as a percentage) where WRED starts marking and dropping traffic.
WRED Maximum Threshold	The configured maximum threshold is the queue depth (as a percentage) above which WRED marks / drops all traffic.
WRED Drop Probability	The configured percentage probability that WRED will mark/drop a packet, when the queue depth is at the maximum threshold. (The drop probability increases linearly from 0 just before the minimum threshold, to this value at the maximum threshold, then goes to 100% for larger queue depths).

Differentiated Services Commands

This section describes the commands you use to configure QOS Differentiated Services (DiffServ).

You configure DiffServ in several stages by specifying three DiffServ components:

1. Class
   a. Creating and deleting classes.
   b. Defining match criteria for a class.
2. Policy
   a. Creating and deleting policies
   b. Associating classes with a policy
   c. Defining policy statements for a policy/class combination
3. Service
   a. Adding and removing a policy to/from an inbound interface

The DiffServ class defines the packet filtering criteria. The attributes of a DiffServ policy define the way the switch processes packets. You can define policy attributes on a per-class instance basis. The switch applies these attributes when a match occurs.

Packet processing begins when the switch tests the match criteria for a packet. The switch applies a policy to a packet when it finds a class match within that policy.

The following rules apply when you create a DiffServ class:

- Each class can contain a maximum of one referenced (nested) class
- Class definitions do not support hierarchical service policies

A given class definition can contain a maximum of one reference to another class. You can combine the reference with other match criteria. The referenced class is truly a reference and not a copy since additions to a referenced class affect all classes that reference it. Changes to any class definition currently referenced by any other class must result in valid class definitions for all derived classes, otherwise the switch rejects the change. You can remove a class reference from a class definition.

The only way to remove an individual match criterion from an existing class definition is to delete the class and re-create it.

Note: The mark possibilities for policing include CoS, IP DSCP, and IP Precedence. While the latter two are only meaningful for IP packet types, CoS marking is allowed for both IP and non-IP packets, since it updates the 802.1p user priority field contained in the VLAN tag of the layer 2 packet header.

diffserv

This command sets the DiffServ operational mode to active. While disabled, the DiffServ configuration is retained and can be changed, but it is not activated. When enabled, DiffServ services are activated.

Format `diffserv`

Mode Global Config

no diffserv

This command sets the DiffServ operational mode to inactive. While disabled, the DiffServ configuration is retained and can be changed, but it is not activated. When enabled, DiffServ services are activated.

Format `no diffserv`

Mode Global Config

DiffServ Class Commands

Use the DiffServ class commands to define traffic classification. To classify traffic, you specify Behavior Aggregate (BA), based on DSCP and Multi-Field (MF) classes of traffic (name, match criteria)

This set of commands consists of class creation/deletion and matching, with the class match commands specifying Layer 3, Layer 2, and general match criteria. The class match criteria are also known as class rules, with a class definition consisting of one or more rules to identify the traffic that belongs to the class.

Note: Once you create a class match criterion for a class, you cannot change or delete the criterion. To change or delete a class match criterion, you must delete and re-create the entire class.

The CLI command root is `class-map`.

class-map

This command defines a DiffServ class of type match-all. When used without any match condition, this command enters the class-map mode. The *`class-map-name`* is a case sensitive alphanumeric string from 1 to 31 characters uniquely identifying an existing DiffServ class.

Note: The class-map-name 'default' is reserved and must not be used.

The class type of `match-all` indicates all of the individual match conditions must be true for a packet to be considered a member of the class.This command may be used without specifying a class type to enter the Class-Map Config mode for an existing DiffServ class.

Note: The optional keywords *[*`{ipv4 | ipv6}`*]* specify the Layer 3 protocol for this class. If not specified, this parameter defaults to `ipv4`. This maintains backward compatibility for configurations defined on systems before IPv6 match items were supported.

Note: The CLI mode is changed to Class-Map Config or Ipv6-Class-Map Config when this command is successfully executed depending on the [{ipv4 | ipv6}] keyword specified.

Format class-map match-all *class-map-name* [{ipv4 | ipv6}]{}

Mode Global Config

no class-map

This command eliminates an existing DiffServ class. The *class-map-name* is the name of an existing DiffServ class. (The class name **default** is reserved and is not allowed here.) This command may be issued at any time; if the class is currently referenced by one or more policies or by any other class, the delete action fails.

Format no class-map *class-map-name*

Mode Global Config

class-map rename

This command changes the name of a DiffServ class. The *class-map-name* is the name of an existing DiffServ class. The *new-class-map-name* parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the class.

Default none

Format class-map rename *class-map-name new-class-map-name*

Mode Global Config

match ethertype

This command adds to the specified class definition a match condition based on the value of the ethertype. The *ethertype* value is specified as one of the following keywords: appletalk, arp, ibmsna, ipv4, ipv6, ipx, mplsmcast, mplsucast, netbios, novell, pppoe, rarp or as a custom EtherType value in the range of 0x0600–0xFFFF.

Format match ethertype {*keyword* | *custom 0x0600-0xFFFF*}

Mode Class-Map Config
Ipv6-Class-Map Config

match any

This command adds to the specified class definition a match condition whereby all packets are considered to belong to the class.

Default none

Format `match any`

Mode Class-Map Config
Ipv6-Class-Map Config

match class-map

This command adds to the specified class definition the set of match conditions defined for another class. The *refclassname* is the name of an existing DiffServ class whose match conditions are being referenced by the specified class definition.

Default none

Format `match class-map refclassname`

Mode Class-Map Config
Ipv6-Class-Map Config

Note:

- The parameters *refclassname* and *class-map-name* can not be the same.
- Only one other class may be referenced by a class.
- Any attempts to delete the *refclassname* class while the class is still referenced by any *class-map-name* fails.
- The combined match criteria of *class-map-name* and *refclassname* must be an allowed combination based on the class type.
- Any subsequent changes to the *refclassname* class match criteria must maintain this validity, or the change attempt fails.
- The total number of class rules formed by the complete reference class chain (including both predecessor and successor classes) must not exceed a platform-specific maximum. In some cases, each removal of a refclass rule reduces the maximum number of available rules in the class definition by one.

no match class-map

This command removes from the specified class definition the set of match conditions defined for another class. The *refclassname* is the name of an existing DiffServ class whose match conditions are being referenced by the specified class definition.

Format `no match class-map refclassname`

Mode Class-Map Config
Ipv6-Class-Map Config

match cos

This command adds to the specified class definition a match condition for the Class of Service value (the only tag in a single tagged packet or the first or outer 802.1Q tag of a double VLAN tagged packet). The value may be from 0 to 7.

Note: This command is not available on the Broadcom 5630x platform.

Default none

Format `match cos 0-7`

Mode Class-Map Config
Ipv6-Class-Map Config

match secondary-cos

This command adds to the specified class definition a match condition for the secondary Class of Service value (the inner 802.1Q tag of a double VLAN tagged packet). The value may be from 0 to 7.

Default none

Format `match secondary-cos 0-7`

Mode Class-Map Config
Ipv6-Class-Map Config

match destination-address mac

This command adds to the specified class definition a match condition based on the destination MAC address of a packet. The *macaddr* parameter is any layer 2 MAC address formatted as six, two-digit hexadecimal numbers separated by colons (e.g., 00:11:22:dd:ee:ff). The *macmask* parameter is a layer 2 MAC address bit mask, which need not be contiguous, and is formatted as six, two-digit hexadecimal numbers separated by colons (e.g., ff:07:23:ff:fe:dc).

Note: This command is not available on the Broadcom 5630x platform.

Default none

Format `match destination-address mac macaddr macmask`

Mode Class-Map Config
Ipv6-Class-Map Config

match dstip

This command adds to the specified class definition a match condition based on the destination IP address of a packet. The *ipaddr* parameter specifies an IP address. The *ipmask* parameter specifies an IP address bit mask and must consist of a contiguous set of leading 1 bits.

Default none

Format `match dstip ipaddr ipmask`

Mode Class-Map Config

match dstip6

This command adds to the specified class definition a match condition based on the destination IPv6 address of a packet.

Default none

Format `match dstip6 destination-ipv6-prefix/prefix-length`

Mode Ipv6-Class-Map Config

match dstl4port

This command adds to the specified class definition a match condition based on the destination layer 4 port of a packet using a single keyword or numeric notation. To specify the match condition as a single keyword, the value for *portkey* is one of the supported port name keywords. The currently supported *portkey* values are: domain, echo, ftp, ftpdata, http, smtp, snmp, telnet, tftp, www. Each of these translates into its equivalent port number. To specify the match condition using a numeric notation, one layer 4 port number is required. The port number is an integer from 0 to 65535.

Default none

Format `match dstl4port {portkey | 0-65535}`

Mode Class-Map Config
Ipv6-Class-Map Config

match ip dscp

This command adds to the specified class definition a match condition based on the value of the IP DiffServ Code Point (DSCP) field in a packet, which is defined as the high-order six bits of the Service Type octet in the IP *header* (the low-order two bits are not checked).

The *dscpval* value is specified as either an integer from 0 to 63, or symbolically through one of the following keywords: af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, ef.

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 Ipv6-Class-Map Config

match ip precedence

This command adds to the specified class definition a match condition based on the value of the IP Precedence field in a packet, which is defined as the high-order three bits of the Service Type octet in the IP header (the low-order five bits are not checked). The precedence value is an integer from 0 to 7.

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 Ipv6-Class-Map Config

match source-address mac

This command adds to the specified class definition a match condition based on the source MAC address of a packet. The *address* parameter is any layer 2 MAC address formatted as six, two-digit hexadecimal numbers separated by colons (e.g., 00:11:22:dd:ee:ff). The *macmask* parameter is a layer 2 MAC address bit mask, which may not be contiguous, and is formatted as six, two-digit hexadecimal numbers separated by colons (e.g., ff:07:23:ff:fe:dc).

Note: This command is not available on the Broadcom 5630x platform.

Default	none
Format	`match source-address mac address macmask`
Mode	Class-Map Config Ipv6-Class-Map Config

match srcip

This command adds to the specified class definition a match condition based on the source IP address of a packet. The *ipaddr* parameter specifies an IP address. The *ipmask* parameter specifies an IP address bit mask and must consist of a contiguous set of leading 1 bits.

Default	none
Format	`match srcip ipaddr ipmask`
Mode	Class-Map Config

match srcip6

This command adds to the specified class definition a match condition based on the source IP address of a packet.

Default	none
Format	`match srcip6 source-ipv6-prefix/prefix-length`
Mode	Ipv6-Class-Map Config

match srcl4port

This command adds to the specified class definition a match condition based on the source layer 4 port of a packet using a single keyword or numeric notation. To specify the match condition as a single keyword notation, the value for *portkey* is one of the supported port name keywords (listed 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
Ipv6-Class-Map Config

match vlan

This command adds to the specified class definition a match condition based on the value of the layer 2 VLAN Identifier field (the only tag in a single tagged packet or the first or outer tag of a double VLAN tagged packet). The VLAN ID is an integer from 0 to 4095.

Note: This command is not available on the Broadcom 5630x platform.

Default none

Format `match vlan 0-4095`

Mode Class-Map Config
Ipv6-Class-Map Config

match secondary-vlan

This command adds to the specified class definition a match condition based on the value of the layer 2 secondary VLAN Identifier field (the inner 802.1Q tag of a double VLAN tagged packet). The secondary VLAN ID is an integer from 0 to 4095.

Note: This command is not available on the Broadcom 5630x platform.

Default none

Format `match secondary-vlan 0-4095`

Mode Class-Map Config
Ipv6-Class-Map Config

DiffServ Policy Commands

Use the DiffServ policy commands to specify traffic conditioning actions, such as policing and marking, to apply to traffic classes

Use the policy commands to associate a traffic class that you define by using the class command set with one or more QoS policy attributes. Assign the class/policy association to an interface to form a service. Specify the policy name when you create the policy.

Each traffic class defines a particular treatment for packets that match the class definition. You can associate multiple traffic classes with a single policy. When a packet satisfies the conditions of more than one class, preference is based on the order in which you add the classes to the policy. The first class you add has the highest precedence.

This set of commands consists of policy creation/deletion, class addition/removal, and individual policy attributes.

Note: The only way to remove an individual policy attribute from a class instance within a policy is to remove the class instance and re-add it to the policy. The values associated with an existing policy attribute can be changed without removing the class instance.

The CLI command root is `policy-map`.

assign-queue

This command modifies the queue id to which the associated traffic stream is assigned. The *queueid* is an integer from 0 to *n*-1, where *n* is the number of egress queues supported by the device.

Format	`assign-queue` *queueid*
Mode	Policy-Class-Map Config
Incompatibilities	Drop

drop

This command specifies that all packets for the associated traffic stream are to be dropped at ingress.

Format	`drop`
Mode	Policy-Class-Map Config
Incompatibilities	Assign Queue, Mark (all forms), Mirror, Police, Redirect

mirror

This command specifies that all incoming packets for the associated traffic stream are copied to a specific egress interface (physical port or LAG).

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 (CoS) value in the priority field of the 802.1p header (the only tag in a single tagged packet or the first or outer 802.1Q tag of a double VLAN tagged packet). If the packet does not already contain this header, one is inserted. The CoS value is an integer from 0 to 7.

Default 1

Format `mark-cos 0-7`

Mode Policy-Class-Map Config

Incompatibilities Drop, Mark IP DSCP, IP Precedence, Police

mark cos-as-sec-cos

This command marks outer VLAN tag priority bits of all packets as the inner VLAN tag priority, marking Cos as Secondary CoS. This essentially means that the inner VLAN tag CoS is copied to the outer VLAN tag CoS.

Format	mark-cos-as-sec-cos
Mode	Policy-Class-Map Config
Incompatibilities	Drop, Mark IP DSCP, IP Precedence, Police

Example: The following shows an example of the command.

```
(switch) (Config-policy-classmap)#mark cos-as-sec-cos
```

mark ip-dscp

This command marks all packets for the associated traffic stream with the specified IP DSCP value.

The *dscpval* value is specified as either an integer from 0 to 63, or symbolically through one of the following keywords: af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, ef.

Format	`mark ip-dscp` *dscpval*
Mode	Policy-Class-Map Config
Incompatibilities	Drop, Mark CoS, Mark IP Precedence, Police

mark ip-precedence

This command marks all packets for the associated traffic stream with the specified IP Precedence value. The IP Precedence value is an integer from 0 to 7.

Note: This command may not be used on IPv6 classes. IPv6 does not have a precedence field.

Format	`mark ip-precedence` *0-7*
Mode	Policy-Class-Map Config
Incompatibilities	Drop, Mark CoS, Mark IP Precedence, Police
Policy Type	In

police-simple

This command is used to establish the traffic policing style for the specified class. The simple form of the **police** command uses a single data rate and burst size, resulting in two outcomes: conform and violate. The conforming data rate is specified in kilobits-per-second (Kbps) and is an integer from 1 to 4294967295. The conforming burst size is specified in kilobytes (KB) and is an integer from 1 to 128.

For each outcome, the only possible actions are drop, set-cos-as-sec-cos, set-cos-transmit, set-sec-cos-transmit, set-dscp-transmit, set-prec-transmit, or transmit. In this simple form of the `police` command, the conform action defaults to transmit and the violate action defaults to drop. These actions can be set with this command once the style has been configured.

For `set-dscp-transmit`, a *dscpval* value is required and is specified as either an integer from 0 to 63, or symbolically through one of the following keywords: af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, ef.

For `set-prec-transmit`, an IP Precedence value is required and is specified as an integer from 0–7.

For `set-cos-transmit` an 802.1p priority value is required and is specified as an integer from 0–7.

Format `police-simple {`*`1-4294967295 1-128`*` conform-action {drop | set-cos-as-sec-cos | set-cos-transmit `*`0-7`*` | set-sec-cos-transmit `*`0-7`*` | set-prec-transmit `*`0-7`*` | set-dscp-transmit `*`0-63`*` | transmit} [violate-action {drop | set-cos-as-sec-cos | set-cos-transmit `*`0-7`*` | set-sec-cos-transmit `*`0-7`*` | set-prec-transmit `*`0-7`*` | set-dscp-transmit `*`0-63`*` | transmit}]}`

Mode Policy-Class-Map Config

Incompatibilities Drop, Mark (all forms)

Example: The following shows an example of the command.

```
(switch) (Config-policy-classmap)#police-simple 1 128 conform-action transmit violate-action drop
```

police-single-rate

This command is the single-rate form of the **police** command and is used to establish the traffic policing style for the specified class. For each outcome, the only possible actions are drop, set-cos-as-sec-cost, set-cos-transmit, set-sec-cos-transmit, set-dscp-transmit, set-prec-transmit, or transmit. In this single-rate form of the **police** command, the conform action defaults to send, the exceed action defaults to drop, and the violate action defaults to drop. These actions can be set with this command once the style has been configured.

Format `police-single-rate {`*`1-4294967295 1-128 1-128`*` conform-action {drop | set-cos-as-sec-cos | set-cos-transmit `*`0-7`*` | set-sec-cos-transmit `*`0-7`*` | set-prec-transmit `*`0-7`*` | set-dscp-transmit `*`0-63`*` | transmit} exceed-action {drop | set-cos-as-sec-cos | set-cos-transmit `*`0-7`*` | set-sec-cos-transmit `*`0-7`*` | set-prec-transmit `*`0-7`*` | set-dscp-transmit `*`0-63`*` | transmit} [violate-action {drop | set-cos-as-sec-cos-transmit | set-cos-transmit `*`0-7`*` | set-sec-cos-transmit `*`0-7`*` | set-prec-transmit `*`0-7`*` | set-dscp-transmit `*`0-63`*` | transmit}]}`

Mode Policy-Class-Map Config

police-two-rate

This command is the two-rate form of the **police** command and is used to establish the traffic policing style for the specified class. For each outcome, the only possible actions are drop, set-cos-as-sec-cos, set-cos-transmit, set-sec-cos-transmit, set-dscp-transmit, set-prec-transmit, or transmit. In this two-rate form of the **police** command, the conform action defaults to send, the exceed action defaults to drop, and the violate action defaults to drop. These actions can be set with this command once the style has been configured.

Format `police-two-rate {1-4294967295 1-4294967295 1-128 1-128 conform-action {drop | set-cos-as-sec-cos | set-cos-transmit 0-7 | set-sec-cos-transmit 0-7 | set-prec-transmit 0-7 | set-dscp-transmit 0-63 | transmit} exceed-action {drop | set-cos-as-sec-cos | set-cos-transmit 0-7 | set-sec-cos-transmit 0-7 | set-prec-transmit 0-7 | set-dscp-transmit 0-63 | transmit} [violate-action {drop | set-cos-as-sec-cos | set-cos-transmit 0-7 | set-sec-cos-transmit 0-7 | set-prec-transmit 0-7 | set-dscp-transmit 0-63 | transmit}]}`

Mode Policy-Class-Map Config

policy-map

This command establishes a new DiffServ policy. The *policyname* parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the policy. The type of policy is specific to the inbound traffic direction as indicated by the in parameter.

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:

Term	*Definition*
Class Name	The name of this class.
Class Type	A class type of all means every match criterion defined for the class is evaluated simultaneously and must all be true to indicate a class match.
L3 Proto	The Layer 3 protocol for this class. Possible values are IPv4 and IPv6.
Match Criteria	The Match Criteria fields are only displayed if they have been configured. Not all platforms support all match criteria values. They are displayed in the order entered by the user. The fields are evaluated in accordance with the class type. The possible Match Criteria fields are: Destination IP Address, Destination Layer 4 Port, Destination MAC Address, Ethertype, Source MAC Address, VLAN, Class of Service, Every, IP DSCP, IP Precedence, IP TOS, Protocol Keyword, Reference Class, Source IP Address, and Source Layer 4 Port.
Values	The values of the Match Criteria.

If you do not specify the Class Name, this command displays a list of all defined DiffServ classes. The following fields are displayed:

Term	*Definition*
Class Name	The name of this class. (Note that the order in which classes are displayed is not necessarily the same order in which they were created.)
Class Type	A class type of all means every match criterion defined for the class is evaluated simultaneously and must all be true to indicate a class match.
Ref Class Name	The name of an existing DiffServ class whose match conditions are being referenced by the specified class definition.

show diffserv

This command displays the DiffServ General Status Group information, which includes the current administrative mode setting as well as the current and maximum number of rows in each of the main DiffServ private MIB tables. This command takes no options.

Format `show diffserv`

Mode Privileged EXEC

Term	*Definition*
DiffServ Admin mode	The current value of the DiffServ administrative mode.
Class Table Size	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:

Term	*Definition*
Policy Name	The name of this policy.
Policy Type	The policy type (only inbound policy definitions are supported for this platform.)

The following information is repeated for each class associated with this policy (only those policy attributes actually configured are displayed):

Term	*Definition*
Assign Queue	Directs traffic stream to the specified QoS queue. This allows a traffic classifier to specify which one of the supported hardware queues are used for handling packets belonging to the class.
Class Name	The name of this class.
Committed Burst Size (KB)	The committed burst size, used in simple policing.
Committed Rate (Kbps)	The committed rate, used in simple policing.
Conform Action	The current setting for the action taken on a packet considered to conform to the policing parameters. This is not displayed if policing is not in use for the class under this policy.
Conform Color Mode	The current setting for the color mode. Policing uses either color blind or color aware mode. Color blind mode ignores the coloration (marking) of the incoming packet. Color aware mode takes into consideration the current packet marking when determining the policing outcome.
Conform COS	The CoS mark value if the conform action is set-cos-transmit.
Conform DSCP Value	The DSCP mark value if the conform action is set-dscp-transmit.
Conform IP Precedence Value	The IP Precedence mark value if the conform action is set-prec-transmit.
Drop	Drop a packet upon arrival. This is useful for emulating access control list operation using DiffServ, especially when DiffServ and ACL cannot co-exist on the same interface.
Exceed Action	The action taken on traffic that exceeds settings that the network administrator specifies.
Exceed Color Mode	The current setting for the color of exceeding traffic that the user may optionally specify.
Mark CoS	The class of service value that is set in the 802.1p header of inbound packets. This is not displayed if the mark cos was not specified.
Mark CoS as Secondary CoS	The secondary 802.1p priority value (second/inner VLAN tag. Same as CoS (802.1p) marking, but the dot1p value used for remarking is picked from the dot1p value in the secondary (i.e. inner) tag of a double-tagged packet.
Mark IP DSCP	The mark/re-mark value used as the DSCP for traffic matching this class. This is not displayed if mark ip description is not specified.
Mark IP Precedence	The mark/re-mark value used as the IP Precedence for traffic matching this class. This is not displayed if mark ip precedence is not specified.
Mirror	Copies a classified traffic stream to a specified egress port (physical port or LAG). This can occur in addition to any marking or policing action. It may also be specified along with a QoS queue assignment. 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	The CoS mark value if the non-conform action is set-cos-transmit.
Non-Conform DSCP Value	The DSCP mark value if the non-conform action is set-dscp-transmit.
Non-Conform IP Precedence Value	The IP Precedence mark value if the non-conform action is set-prec-transmit.

Term	*Definition*
Peak Rate	Guarantees a committed rate for transmission, but also transmits excess traffic bursts up to a user-specified peak rate, with the understanding that a downstream network element (such as the next hop's policer) might drop this excess traffic. Traffic is held in queue until it is transmitted or dropped (per type of queue depth management.) Peak rate shaping can be configured for the outgoing transmission stream for an AP traffic class (although average rate shaping could also be used.)
Peak Burst Size	(PBS). The network administrator can set the PBS as a means to limit the damage expedited forwarding traffic could inflict on other traffic (e.g., a token bucket rate limiter) Traffic that exceeds this limit is discarded.
Policing Style	The style of policing, if any, used (simple).
Redirect	Forces a classified traffic stream to a specified egress port (physical port or LAG). This can occur in addition to any marking or policing action. It may also be specified along with a QoS queue assignment. 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:

Term	Definition
Policy Name	The name of this policy. (The order in which the policies are displayed is not necessarily the same order in which they were created.)
Policy Type	The policy type (Only inbound is supported).
Class Members	List of all class names associated with this policy.

Example: The following shows example CLI display output including the mark-cos-as-sec-cos option specified in the policy action.

```
(Routing) #show policy-map p1
Policy Name..................................... p1
Policy Type..................................... In
Class Name...................................... c1
Mark CoS as Secondary CoS...................... Yes
```

Example: The following shows example CLI display output including the mark-cos-as-sec-cos action used in the policing (simple-police, police-single-rate, police two-rate) command.

```
(Routing) #show policy-map p2
Policy Name..................... p2
Policy Type..................... In
Class Name...................... c2
Policing Style.................. Police Two Rate
Committed Rate.................. 1
Committed Burst Size............ 1
Peak Rate....................... 1
Peak Burst Size................. 1
Conform Action.................. Mark CoS as Secondary CoS
Exceed Action................... Mark CoS as Secondary CoS
Non-Conform Action.............. Mark CoS as Secondary CoS
Conform Color Mode.............. Blind
Exceed Color Mode............... Blind
```

show diffserv service

This command displays policy service information for the specified interface and direction. The slot/port parameter specifies a valid slot/port number for the system.

Format `show diffserv service slot/port in`

Mode Privileged EXEC

Term	*Definition*
DiffServ Admin Mode	The current setting of the DiffServ administrative mode. An attached policy is only in effect on an interface while DiffServ is in an enabled mode.
Interface	*slot/port*
Direction	The traffic direction of this interface service.
Operational Status	The current operational status of this DiffServ service interface.
Policy Name	The name of the policy attached to the interface in the indicated direction.
Policy Details	Attached policy details, whose content is identical to that described for the show policy-map *policymapname* command (content not repeated here for brevity).

show diffserv service brief

This command displays all interfaces in the system to which a DiffServ policy has been attached. The inbound direction parameter is optional.

Format `show diffserv service brief [in]`

Mode Privileged EXEC

Term	*Definition*
DiffServ Mode	The current setting of the DiffServ administrative mode. An attached policy is only active on an interface while DiffServ is in an enabled mode.

The following information is repeated for interface and direction (only those interfaces configured with an attached policy are shown):

Term	*Definition*
Interface	*slot/port*
Direction	The traffic direction of this interface service.
OperStatus	The current operational status of this DiffServ service interface.
Policy Name	The name of the policy attached to the interface in the indicated direction.

show policy-map interface

This command displays policy-oriented statistics information for the specified interface and direction. The slot/port parameter specifies a valid interface for the system.

Note: This command is only allowed while the DiffServ administrative mode is enabled.

Format `show policy-map interface slot/port [in]`

Mode Privileged EXEC

Term	*Definition*
Interface	*slot/port*
Direction	The traffic direction of this interface service.
Operational Status	The current operational status of this DiffServ service interface.
Policy Name	The name of the policy attached to the interface in the indicated direction.

The following information is repeated for each class instance within this policy:

Term	*Definition*
Class Name	The name of this class instance.
In Discarded Packets	A count of the packets discarded for this class instance for any reason due to DiffServ treatment of the traffic class.

show service-policy

This command displays a summary of policy-oriented statistics information for all interfaces in the specified direction.

Format `show service-policy in`

Mode Privileged EXEC

The following information is repeated for each interface and direction (only those interfaces configured with an attached policy are shown):

Term	*Definition*
Interface	*slot/port*
Operational Status	The current operational status of this DiffServ service interface.
Policy Name	The name of the policy attached to the interface.

MAC Access Control List Commands

This section describes the commands you use to configure MAC Access Control List (ACL) settings. MAC ACLs ensure that only authorized users have access to specific resources and block any unwarranted attempts to reach network resources.

The following rules apply to MAC ACLs:

- The maximum number of ACLs you can create is hardware dependent. The limit applies to all ACLs, regardless of type.
- The system supports only Ethernet II frame types.
- The maximum number of rules per MAC ACL is hardware dependent.
- 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} (MAC ACL)

This command creates a new rule for the current MAC access list. Each rule is appended to the list of configured rules for the list.

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.

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 14: Ethertype Keyword and 4-digit Hexadecimal Value

Ethertype Keyword	*Corresponding Value*
appletalk	0x809B
arp	0x0806
ibmsna	0x80D5
ipv4	0x0800
ipv6	0x86DD
ipx	0x8037
mplsmcast	0x8848
mplsucast	0x8847
netbios	0x8191
novell	0x8137, 0x8138
pppoe	0x8863, 0x8864

Table 14: Ethertype Keyword and 4-digit Hexadecimal Value

Ethertype Keyword	*Corresponding Value*
rarp	0x8035

The `vlan` and `cos` parameters refer to the VLAN identifier and 802.1p user priority fields, respectively, of the VLAN tag. For packets containing a double VLAN tag, this is the first (or outer) tag.

The `time-range` parameter allows imposing time limitation on the MAC ACL rule as defined by the parameter *time-range-name*. If a time range with the specified name does not exist and the MAC ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied immediately. If a time range with specified name exists and the MAC ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied when the time-range with specified name becomes active. The ACL rule is removed when the time-range with specified name becomes inactive. For information about configuring time ranges, see "Time Range Commands for Time-Based ACLs" on page 835.

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] [time-range time-range-name] [assign-queue queue-id]] [{mirror | redirect} slot/port]`

Mode Mac-Access-List Config

mac access-group

This command either attaches a specific MAC Access Control List (ACL) identified by *name* to an interface or range of interfaces, or associates it with a VLAN ID, in a given direction. The *name* parameter must be the name of an existing MAC ACL.

An optional sequence number may be specified to indicate the order of this mac access list relative to other mac access lists already assigned to this interface and direction. A lower number indicates higher precedence order. If a sequence number is already in use for this interface and direction, the specified mac access list replaces the currently attached mac access list using that sequence number. If the sequence number is not specified for this command, a sequence number that is one greater than the highest sequence number currently in use for this interface and direction is used.

This command specified in Interface Config mode only affects a single interface, whereas the Global Config mode setting is applied to all interfaces. The VLAN keyword is only valid in the Global Config mode. The 'Interface Config' mode command is only available on platforms that support independent per-port class of service queue configuration.

Note: The `out` option may or may not be available, depending on the platform.

Format `mac access-group` *name* `[vlan` *vlan-id]* `[in|out] [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-group` *name* `[vlan` *vlan-id*`] 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

Term	*Definition*
Rule Number	The ordered rule number identifier defined within the MAC ACL.
Action	The action associated with each rule. The possible values are Permit or Deny.
Source MAC Address	The source MAC address for this rule.

Term	*Definition*
Destination MAC Address	The destination MAC address for this rule.
Ethertype	The Ethertype keyword or custom value for this rule.
VLAN ID	The VLAN identifier value or range for this rule.
COS	The COS (802.1p) value for this rule.
Log	Displays when you enable logging for the rule.
Assign Queue	The queue identifier to which packets matching this rule are assigned.
Mirror Interface	On Broadcom 5650x platforms, the unit/slot/port to which packets matching this rule are copied.
Redirect Interface	On Broadcom 5650x platforms, the slot/port to which packets matching this rule are forwarded.
Time Range Name	Displays the name of the time-range if the MAC ACL rule has referenced a time range.
Rule Status	Status (Active/Inactive) of the MAC ACL rule.

IP Access Control List Commands

This section describes the commands you use to configure IP Access Control List (ACL) settings. IP ACLs ensure that only authorized users have access to specific resources and block any unwarranted attempts to reach network resources.

The following rules apply to IP ACLs:

- DWS-4000 software does not support IP ACL configuration for IP packet fragments.
- The maximum number of ACLs you can create is hardware dependent. The limit applies to all ACLs, regardless of type.
- The maximum number of rules per IP ACL is hardware dependent.
- 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 15 describes the parameters for the `access-list` command.

IP Standard ACL:

Format `access-list` *1-99* {deny | permit} {every | *srcip srcmask*} [log] [time-range *time-range-name*][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][time-range *time-range-name*][assign-queue *queue-id*] [{mirror | redirect} *unit/slot/port*]

Mode Global Config

Table 15: 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.
[time-range *time-range-name*]	Allows imposing time limitation on the ACL rule as defined by the parameter *time-range-name*. If a time range with the specified name does not exist and the ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied immediately. If a time range with specified name exists and the ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied when the time-range with specified name becomes active. The ACL rule is removed when the time-range with specified name becomes inactive. For information about configuring time ranges, see "Time Range Commands for Time-Based ACLs" on page 835.
[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-list

This command creates an extended IP Access Control List (ACL) identified by *name*, consisting of classification fields defined for the IP header of an IPv4 frame. The *name* parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the IP access list.

If an IP ACL by this name already exists, this command enters IPv4-Access-List config mode to allow updating the existing IP ACL.

Note: The CLI mode changes to IPv4-Access-List Config mode when you successfully execute this command.

Format ip access-list *name*

Mode Global Config

no ip access-list

This command deletes the IP ACL identified by name from the system.

Format no ip access-list *name*

Mode Global Config

ip access-list rename

This command changes the name of an IP Access Control List (ACL). The *name* parameter is the names of an existing IP ACL. The *newname* parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the IP access list.

This command fails is an IP ACL by the name *newname* already exists.

Format ip access-list rename *name newname*

Mode Global Config

{deny | permit} (IP ACL)

This command creates a new rule for the current IP access list. Each rule is appended to the list of configured rules for the list.

Note: The 'no' form of this command is not supported, since the rules within an IP ACL cannot be deleted individually. Rather, the entire IP ACL must be deleted and re-specified.

Note: An implicit 'deny all' IP rule always terminates the access list.

A rule may either deny or permit traffic according to the specified classification fields. At a minimum, either the every keyword or the protocol, source address, and destination address values must be specified. The source and destination IP address fields may be specified using the keyword `any` to indicate a match on any value in that field. The remaining command parameters are all optional, but the most frequently used parameters appear in the same relative order as shown in the command format.

The `time-range` parameter allows imposing time limitation on the IP ACL rule as defined by the specified time range. If a time range with the specified name does not exist and the ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied immediately. If a time range with specified name exists and the ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied when the time-range with specified name becomes active. The ACL rule is removed when the time-range with specified name becomes inactive. For information about configuring time ranges, see "Time Range Commands for Time-Based ACLs" on page 835.

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.

Format {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] [time-range *time-range-name*] [assign-queue *queue-id*] [{mirror | redirect} *unit/slot/port*]

Mode Ipv4-Access-List Config

ip access-group

This command either attaches a specific IP ACL identified by *accesslistnumber* to an interface, range of interfaces, or all interfaces; or associates it with a VLAN ID in a given direction. The parameter `name` is the name of the Access Control List.

An optional sequence number may be specified to indicate the order of this IP access list relative to other IP access lists already assigned to this interface and direction. A lower number indicates higher precedence order. If a sequence number is already in use for this interface and direction, the specified access list replaces the currently attached IP access list using that sequence number. If the sequence number is not specified for this command, a sequence number that is one greater than the highest sequence number currently in use for this interface and direction is used.

Note: You should be aware that the `out` option may or may not be available, depending on the platform.

Default none

Format `ip access-group accesslistnumber name [vlan vlan-id] in | out[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 [vlan vlan-id] in`

Mode
- Interface Config
- Global 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

Use this command to view summary information about all IP ACLs configured on the switch. To view more detailed information about a specific access list, specify the ACL number or name that is used to identify the IP ACL.

Format `show ip access-lists [accesslistnumber | name]`

Mode Privileged EXEC

Term	*Definition*
ACL ID/Name	Identifies the configured ACL number or name.
Rules	Identifies the number of rules configured for the ACL.
Direction	Shows whether the ACL is applied to traffic coming into the interface (ingress) or leaving the interface (egress).
Interface(s)	Identifies the interface(s) to which the ACL is applied (ACL interface bindings).

Term	*Definition*
VLAN(s)	Identifies the VLANs to which the ACL is applied (ACL VLAN bindings).

If you specify an IP ACL number or name, the following information displays:

Note: Only the access list fields that you configure are displayed.

Term	*Definition*
Rule Number	The number identifier for each rule that is defined for the IP ACL.
Action	The action associated with each rule. The possible values are Permit or Deny.
Match All	Indicates whether this access list applies to every packet. Possible values are True or False.
Protocol	The protocol to filter for this rule.
Source IP Address	The source IP address for this rule.
Source IP Mask	The source IP Mask for this rule.
Source L4 Port Keyword	The source port for this rule.
Destination IP Address	The destination IP address for this rule.
Destination IP Mask	The destination IP Mask for this rule.
Destination L4 Port Keyword	The destination port for this rule.
IP DSCP	The value specified for IP DSCP.
IP Precedence	The value specified IP Precedence.
IP TOS	The value specified for IP TOS.
Log	Displays when you enable logging for the rule.
Assign Queue	The queue identifier to which packets matching this rule are assigned.
Mirror Interface	The unit/slot/port to which packets matching this rule are copied.
Redirect Interface	The unit/slot/port to which packets matching this rule are forwarded.
Time Range Name	Displays the name of the time-range if the IP ACL rule has referenced a time range.
Rule Status	Status (Active/Inactive) of the IP ACL rule.

show access-lists

This command displays IP ACLs, IPv6 ACLs, and MAC access control lists information for a designated interface and direction.

Format `show access-lists interface slot/port in`

Mode Privileged EXEC

Term	*Definition*
ACL Type	Type of access list (IP, IPv6, or MAC).
ACL ID	Access List name for a MAC or IPv6 access list or the numeric identifier for an IP access list.
Sequence Number	An optional sequence number may be specified to indicate the order of this access list relative to other access lists already assigned to this interface and direction. A lower number indicates higher precedence order. If a sequence number is already in use for this interface and direction, the specified access list replaces the currently attached access list using that sequence number. If the sequence number is not specified by the user, a sequence number that is one greater than the highest sequence number currently in use for this interface and direction is used. Valid range is (1 to 4294967295).

IPv6 Access Control List Commands

This section describes the commands you use to configure IPv6 Access Control List (ACL) settings. IPv6 ACLs ensure that only authorized users have access to specific resources and block any unwarranted attempts to reach network resources.

The following rules apply to IPv6 ACLs:

- The maximum number of ACLs you create is 100, regardless of type.
- The system supports only Ethernet II frame types.
- The maximum number of rules per IPv6 ACL is hardware dependent.

ipv6 access-list

This command creates an IPv6 Access Control List (ACL) identified by *name*, consisting of classification fields defined for the IP header of an IPv6 frame. The *name* parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the IPv6 access list.

If an IPv6 ACL by this name already exists, this command enters IPv6-Access-List config mode to allow updating the existing IPv6 ACL.

Note: The CLI mode changes to IPv6-Access-List Config mode when you successfully execute this command.

Format `ipv6 access-list name`

Mode Global Config

no ipv6 access-list

This command deletes the IPv6 ACL identified by *name* from the system.

Format `no ipv6 access-list name`

Mode Global Config

ipv6 access-list rename

This command changes the name of an IPv6 ACL. The *name* parameter is the name of an existing IPv6 ACL. The *newname* parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the IPv6 access list.

This command fails is an IPv6 ACL by the name *newname* already exists.

Format `ipv6 access-list rename name newname`

Mode Global Config

{deny | permit} (IPv6)

This command creates a new rule for the current IPv6 access list. Each rule is appended to the list of configured rules for the list.

Note: The no form of this command is not supported, since the rules within an IPv6 ACL cannot be deleted individually. Rather, the entire IPv6 ACL must be deleted and respecified.

Note: An implicit deny all IPv6 rule always terminates the access list.

A rule may either deny or permit traffic according to the specified classification fields. At a minimum, either the every keyword or the protocol, source address, and destination address values must be specified. The source and destination IPv6 address fields may be specified using the keyword any to indicate a match on any value in that field. The remaining command parameters are all optional, but the most frequently used parameters appear in the same relative order as shown in the command format.

The time-range parameter allows imposing time limitation on the IPv6 ACL rule as defined by the parameter *time-range-name*. If a time range with the specified name does not exist and the IPv6 ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied immediately. If a time range with specified name exists and the IPv6 ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied when the time-range with specified name becomes active. The ACL rule is removed when the time-range with specified name becomes inactive. For information about configuring time ranges, see "Time Range Commands for Time-Based ACLs" on page 835.

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.

Format {deny | permit} {every | {{icmpv6 | ipv6 | tcp | udp | *number*}[log] [time-range *time-range-name*] [assign-queue *queue-id*] [{mirror | redirect} slot/port]

Mode IPv6-Access-List Config

ipv6 traffic-filter

This command either attaches a specific IPv6 ACL identified by *name* to an interface or range of interfaces, or associates it with a VLAN ID in a given direction. The *name* parameter must be the name of an existing IPv6 ACL.

An optional sequence number may be specified to indicate the order of this mac access list relative to other IPv6 access lists already assigned to this interface and direction. A lower number indicates higher precedence order. If a sequence number is already in use for this interface and direction, the specifiedIPv6 access list replaces the currently attached IPv6 access list using that sequence number. If the sequence number is not specified for this command, a sequence number that is one greater than the highest sequence number currently in use for this interface and direction is used.

This command specified in Interface Config mode only affects a single interface, whereas the Global Config mode setting is applied to all interfaces. The vlan keyword is only valid in the Global Config mode. The Interface Config mode command is only available on platforms that support independent per-port class of service queue configuration.

Note: You should be aware that the *out* option may or may not be available, depending on the platform.

Format `ipv6 traffic-filter name [vlan vlan-id] {in | out} [sequence 1-4294967295]`

Modes
- Global Config
- Interface Config

no ipv6 traffic-filter

This command removes an IPv6 ACL identified by *name* from the interface(s) in a given direction.

Format `no ipv6 traffic-filter name [vlan vlan-id] in [sequence 1-4294967295]`

Modes
- Global Config
- Interface Config

show ipv6 access-lists

This command displays an IPv6 access list and all of the rules that are defined for the IPv6 ACL. Use the *[name]* parameter to identify a specific IPv6 ACL to display.

Format `show ipv6 access-lists [name]`

Mode Privileged EXEC

Term	*Definition*
Rule Number	The ordered rule number identifier defined within the IPv6 ACL.
Action	The action associated with each rule. The possible values are Permit or Deny.
Match All	Indicates whether this access list applies to every packet. Possible values are True or False.
Protocol	The protocol to filter for this rule.
Source IP Address	The source IP address for this rule.
Source L4 Port Keyword	The source port for this rule.
Destination IP Address	The destination IP address for this rule.
Destination L4 Port Keyword	The destination port for this rule.
IP DSCP	The value specified for IP DSCP.
Flow Label	The value specified for IPv6 Flow Label.
Log	Displays when you enable logging for the rule.
Assign Queue	The queue identifier to which packets matching this rule are assigned.
Mirror Interface	The slot/port to which packets matching this rule are copied.
Redirect Interface	The slot/port to which packets matching this rule are forwarded.
Time Range Name	Displays the name of the time-range if the IPv6 ACL rule has referenced a time range.
Rule Status	Status (Active/Inactive) of the IPv6 ACL rule.

Time Range Commands for Time-Based ACLs

Time-based ACLs allow one or more rules within an ACL to be based on time. Each ACL rule within an ACL except for the implicit *deny all* rule can be configured to be active and operational only during a specific time period. The time range commands allow you to define specific times of the day and week in order to implement time-based ACLs. The time range is identified by a name and can then be referenced by an ACL rule defined with in an ACL.

time-range

Use this command to create a time range identified by *name*, consisting of one absolute time entry and/or one or more periodic time entries. The *name* parameter is a case-sensitive, alphanumeric string from 1 to 31 characters that uniquely identifies the time range. An alpha-numeric string is defined as consisting of only alphabetic, numeric, dash, underscore, or space characters.

If a time range by this name already exists, this command enters Time-Range config mode to allow updating the time range entries.

Note: When you successfully execute this command, the CLI mode changes to Time-Range Config mode.

Format `time-range` *name*

Mode Global Config

no time-range

This command deletes a time-range identified by *name*.

Format `no time-range` *name*

Mode Global Config

absolute

Use this command to add an absolute time entry to a time range. Only one absolute time entry is allowed per time-range. The *time* parameter is based on the currently configured time zone.

The *[start time date]* parameters indicate the time and date at which the configuration that referenced the time range starts going into effect. The time is expressed in a 24-hour clock, in the form of hours:minutes. For example, 8:00 is 8:00 am and 20:00 is 8:00 pm. The date is expressed in the format day month year. If no start time and date are specified, the configuration statement is in effect immediately.

The *[end time date]* parameters indicate the time and date at which the configuration that referenced the time range is no longer in effect. The end time and date must be after the start time and date. If no end time and date are specified, the configuration statement is in effect indefinitely.

Format *absolute {[start time date] [end time date]}*

Mode Time-Range Config

no absolute

This command deletes the absolute time entry in the time range

Format `no absolute`

Mode Time-Range Config

periodic

Use this command to add a periodic time entry to a time range. The *time* parameter is based off of the currently configured time zone.

The first occurrence of the *days-of-the-week* argument is the starting day(s) from which the configuration that referenced the time range starts going into effect. The second occurrence is the ending day or days from which the configuration that referenced the time range is no longer in effect. If the end *days-of-the-week* are the same as the start, they can be omitted

This argument can be any single day or combinations of days: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday. Other possible values are:

- daily — Monday through Sunday
- weekdays — Monday through Friday
- weekend — Saturday and Sunday

If the ending days of the week are the same as the starting days of the week, they can be omitted.

The first occurrence of the `time` argument is the starting hours:minutes which the configuration that referenced the time range starts going into effect. The second occurrence is the ending hours:minutes at which the configuration that referenced the time range is no longer in effect.

The hours:minutes are expressed in a 24-hour clock. For example, 8:00 is 8:00 am and 20:00 is 8:00 pm.

Format *periodic {days-of-the-week time} to {[days-of-the-week] time}*

Mode Time-Range Config

no periodic

This command deletes a periodic time entry from a time range

Format *no periodic {days-of-the-week time} to {[days-of-the-week] time}*

Mode Time-Range Config

show time-range

Use this command to display a time range and all the absolute/periodic time entries that are defined for the time range. Use the *name* parameter to identify a specific time range to display. When *name* is not specified, all the time ranges defined in the system are displayed.

Format `show time-range`

Mode Privileged EXEC

Term	*Definition*
Number of Time Ranges	Number of time ranges configured in the system.
Time Range Name	Name of the time range.
Time Range Status	Status of the time range (active/inactive)
Absolute start	Start time and day for absolute time entry.
Absolute end	End time and day for absolute time entry.
Periodic Entries	Number of periodic entries in a time-range.
Periodic start	Start time and day for periodic entry.
Periodic end	End time and day for periodic entry.

Auto-Voice over IP Commands

This section describes the commands you use to configure Auto-Voice over IP (VoIP) commands. The Auto-VoIP feature explicitly matches VoIP streams in Ethernet switches and provides them with a better class-of-service than ordinary traffic. When you enable the Auto-VoIP feature on an interface, the interface scans incoming traffic for the following call-control protocols:

- Session Initiation Protocol (SIP)
- H.323
- Skinny Client Control Protocol (SCCP)

When a call-control protocol is detected, the switch assigns the traffic in that session to the highest CoS queue, which is generally used for time-sensitive traffic.

auto-voip all

Use this command to enable VoIP Profile on the interfaces of the switch.

Default disabled

Format `auto-voip all`

Mode Global Config

no auto-voip all

Use this command to disable VoIP Profile on the interfaces of the switch.

Format `no auto-voip all`

Mode Global Config

auto-voip

Use this command to enable VoIP Profile on an interface or range of interfaces.

Default disabled

Format `auto-voip`

Mode Interface Config

no auto-voip

Use this command to disable VoIP Profile on the interface.

Format `no auto-voip all`

Mode Interface Config

show auto-voip

Use this command to display the VoIP Profile settings on the interface or interfaces of the switch.

Format `show auto-voip interface {slot/port | all}`

Mode Privileged EXEC

Field	*Description*
AutoVoIP Mode	The Auto VoIP mode on the interface.
Traffic Class	The CoS Queue or Traffic Class to which all VoIP traffic is mapped to. This is not configurable and defaults to the highest CoS queue available in the system for data traffic.

iSCSI Optimization Commands

This section describes commands you use to monitor iSCSI sessions and prioritize iSCSI packets. iSCSI Optimization provides a means of giving traffic between iSCSI initiator and target systems special Quality of Service (QoS) treatment. This is accomplished by monitoring traffic to detect packets used by iSCSI stations to establish iSCSI sessions and connections. Data from these exchanges is used to create classification rules that assign the traffic between the stations to a configured traffic class. Packets in the flow are queued and scheduled for egress on the destination port based on these rules.

iscsi aging time

This command sets the aging time for iSCSI sessions. Behavior when changing aging time:

- When aging time is increased, current sessions will be timed out according to the new value.
- When aging time is decreased, any sessions that have been dormant for a time exceeding the new setting will be immediately deleted from the table. All other sessions will continue to be monitored against the new time out value.

Default `10 minutes`

Format `iscsi aging time` *`time`*

Mode Global Config

Parameter	*Description*
time	The number of minutes a session must be inactive prior to its removal. Range: 1–43,200.

Example: The following example sets the aging time for iSCSI sessions to 100 minutes.

```
(switch)(config)#iscsi aging time 100
```

no iscsi aging time

Use the `no` form of the command to reset the aging time value to the default value.

Format `no iscsi aging time`

Mode Global Config

iscsi cos

This command sets the quality of service profile that will be applied to iSCSI flows. iSCSI flows are assigned by default to the highest VPT/DSCP mapped to the highest queue not used for stack management. The user should also take care of configuring the relevant Class of Service parameters for the queue in order to complete the setting.

Setting the VPT/DSCP sets the QoS profile which determines the egress queue to which the frame is mapped. The switch default setting for egress queues scheduling is Weighted Round Robin (WRR).

You may complete the QoS setting by configuring the relevant ports to work in other scheduling and queue management modes via the Class of Service settings. Depending on the platform, these choices may include strict priority for the queue used for iSCSI traffic. The downside of strict priority is that, in certain circumstances (under heavy high priority traffic), other lower priority traffic may get starved. In WRR the queue to which the flow is assigned to can be set to get the required percentage.

Format `iscsi cos {vpt vpt | dscp dscp} [remark]`

Mode Global Config

Parameter	*Description*
vpt/dscp	The VLAN Priority Tag or DSCP to assign iSCSI session packets.
remark	Mark the iSCSI frames with the configured VPT/DSCP when egressing the switch.

Example: The following example sets the quality of service profile that will be applied to iSCSI flows.

```
(switch)(config)#iscsi cos vpt 5 remark
```

no iscsi cos

Use the `no` form of the command to return to the default.

Format `no iscsi cos`

Mode Global Config

iscsi enable

This command globally enables iSCSI awareness.

Default `disabled`

Format `iscsi enable`

Mode Global Config

Example: The following example enables iSCSI awareness.

```
(switch)(config)#iscsi enable
```

no iscsi enable

This command disables iSCSI awareness. When you use the `no iscsi enable` command, iSCSI resources will be released.

Format `no iscsi enable`

Mode Global Config

iscsi target port

This command configures an iSCSI target port and, optionally, a target system's IP address and IQN name. When working with private iSCSI ports (not IANA-assigned ports 3260/860), it is recommended to specify the target IP address as well, so that the switch will only snoop frames with which the TCP destination port is one of the configured TCP ports, and the destination IP is the target's IP address. This way the CPU will not be falsely loaded by non-iSCSI flows (if by chance other applications also choose to use these un-reserved ports.

When a port is already defined and not bound to an IP address, and you want to bind it to an IP address, you should first remove it by using the `no` form of the command and then add it again, this time together with the relevant IP address.

Target names are only for display when using the **show iscsi** command. These names are not used to match with the iSCSI session information acquired by snooping.

A maximum of 16 TCP ports can be configured either bound to IP or not.

Default iSCSI well-known ports 3260 and 860 are configured as default but can be removed as any other configured target.

Format `iscsi target port` *`tcp-port-1 [tcp-port-2...tcp-port-16]`* `[address` *`ip-address]`* `[name` *`targetname`*`]`

Mode Global Config

Parameter	*Description*
tcp-port-n	TCP port number or list of TCP port numbers on which the iSCSI target listens to requests. Up to 16 TCP ports can be defined in the system in one command or by using multiple commands.
ip-address	IP address of the iSCSI target. When the no form of this command is used, and the tcp port to be deleted is one bound to a specific IP address, the address field must be present.
targetname	iSCSI name of the iSCSI target. The name can be statically configured; however, it can be obtained from iSNS or from sendTargets response. The initiator must present both its iSCSI Initiator Name and the iSCSI Target Name to which it wishes to connect in the first login request of a new session or connection.

Example: The following example configures TCP Port 49154 to target IP address 172.16.1.20.

```
(switch)(config)#iscsi target port 49154 address 172.16.1.20
```

no iscsi target port

Use the no form of the command to delete an iSCSI target port, address, and name.

show iscsi

This command displays the iSCSI settings.

Format	show iscsi
Mode	Privileged EXEC

Example: The following are examples of the commands used for iSCSI.

Example #1: Show iSCSI (Default Configuration)

```
(switch)#show iscsi
iSCSI disabled
iSCSI vpt is 5, remark
Session aging time: 10 min
Maximum number of sessions is 192
-----------------------------------------
iSCSI Targets and TCP ports:
-----------------------------------------
TCP Port   Target IP Address     Name
860        Not Configured        Not Configured
3260       Not Configured        Not Configured
```

Example #2: Enable iSCSI.

```
(switch)#configure
(switch)(config)#iscsi enable
```

Example #3: Show iSCSI (After Enable)

The following configuration detects iSCSI sessions and connections established using TCP ports 3260 or 860. Packets sent on detected iSCSI TCP connections are assigned to traffic class 2 (see the CoS configuration shown below). Since remark is enabled, the packets are marked with IEEE 802.1p priority to 5 before transmission.

```
(switch)#show iscsi
iscsi enabled
iSCSI vpt is 5, remark
Session aging time: 10 min
Maximum number of sessions is 192
-----------------------------------------
iSCSI Targets and TCP ports:
-----------------------------------------
TCP Port   Target IP Address     Name
860        Not Configured        Not Configured
3260       Not Configured        Not Configured

(switch)#show classofservice dot1p-mapping
User Priority    Traffic Class
-------------    -------------
       0               1
```

```
1               0
2               0
3               1
4               2
5               2
6               3
6               3
```

show iscsi sessions

This command displays the iSCSI sessions.

Default	If not specified, sessions are displayed in short mode (not detailed).
Format	show iscsi sessions [detailed]
Mode	Privileged EXEC

Example: The following example displays the iSCSI sessions.

```
(switch) # show iscsi sessions
Target: iqn.1993-11.com.disk-vendor:diskarrays.sn.45678
-----------------------------------------------------------
Initiator: iqn.1992-04.com.os-vendor.plan9:cdrom.12
ISID: 11
Initiator: iqn.1995-05.com.os-vendor.plan9:cdrom.10
ISID: 222
-----------------------------------------------------------
Target: iqn.103-1.com.storage-vendor:sn.43338.
storage.tape:sys1.xyz
Session 3:
Initiator: iqn.1992-04.com.os-vendor.plan9:cdrom.12
Session 4:
Initiator: iqn.1995-05.com.os-vendor.plan9:cdrom.10
-----------------------------------------------------------

(switch)# show iscsi sessions detailed
Target: iqn.1993-11.com.disk-vendor:diskarrays.sn.45678
-----------------------------------------------------------
Session 1:

Initiator: iqn.1992-04.com.os
vendor.plan9:cdrom.12.storage:sys1.xyz
-----------------------------------------------------------
Time started: 17-Jul-2008 10:04:50
Time for aging out: 10 min
ISID: 11

Initiator         Initiator         Target            Target
IP address        TCP port          IP address        IP port
172.16.1.3        49154             172.16.1.20       30001
172.16.1.4        49155             172.16.1.21       30001
172.16.1.5        49156             172.16.1.22       30001

Session 2:
-----------------------------------------------------------
```

```
Initiator: iqn.1995-05.com.os-vendor.plan9:cdrom.10
Time started: 17-Aug-2008  21:04:50
Time for aging out: 2 min
ISID: 22
Initiator         Initiator         Target            Target
IP address        TCP port          IP address        IP port
172.16.1.30       49200             172.16.1.20       30001
172.16.1.30       49201             172.16.1.21       30001
```

Section 10: IP Multicast Commands

This chapter describes the IP Multicast commands available in the DWS-4000 CLI.

The IP Multicast Commands chapter contains the following sections:

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

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

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. This command can be used to configure a single interface or a range of interfaces.

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.

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.

Format `no ip multicast`

Mode Global Config

ip multicast ttl-threshold

This command is specific to IPv4. Use this command to apply the given Time-to-Live threshold value to a routing interface or range of interfaces. The `ttl-threshold` is the TTL threshold which is to be applied to the multicast Data packets which are to be forwarded from the interface. This command sets the Time-to-Live threshold value such that any data packets forwarded over the interface having TTL value above the configured value are dropped. The value for `ttl-threshold` ranges 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 `ttl-threshold` to a routing interface. The `ttl-threshold` 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

show ip mcast

This command displays the system-wide multicast information.

Format `show ip mcast`

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
Admin Mode	The administrative status of multicast. Possible values are enabled or disabled.
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.
Protocol	The multicast protocol running on the router. Possible values are PIMDM, PIMSM, or DVMRP.
Multicast Forwarding Cache Entry Count	The number of entries in the multicast forwarding cache.

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

Term	*Definition*
Interface	*slot/port*
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

Term	*Definition*
Interface	*slot/port*
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

If you use the *detail* parameter, the command displays the following fields:

Term	*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:

Term	*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 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

Term	*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:

Term	*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:

Term	*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.

DVMRP Commands

This section describes the Distance Vector Multicast Routing Protocol (DVMRP) commands.

ip dvmrp

This command sets administrative mode of DVMRP in the router to active.

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 or range of interfaces. 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 or range of interfaces 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

Term	*Definition*
Admin Mode	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.

Term	*Definition*
Interface	*slot/port*
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

Term	*Definition*
Interface Mode	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.

The following field is displayed only when DVMRP is operational on the interface.

Term	*Definition*
Generation ID	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.

Term	*Definition*
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

Term	*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.

Term	*Definition*
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.
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

Term	*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

Term	*Definition*
Group IP	The multicast Address that is pruned.
Source IP	The IP address of the source that has pruned.
Source Mask	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)	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

Term	*Definition*
Source Address	The multicast address of the source group.
Source Mask	The IP Mask for the source group.
Upstream Neighbor	The IP address of the neighbor which is the source for the packets for a specified multicast address.
Interface	The interface used to receive the packets sent by the sources.
Metric	The distance in hops to the source subnet. This field has a different meaning than the Interface Metric field.
Expiry Time (secs)	The expiry time in seconds, which is the time left for this route to age out.
Up Time (secs)	The time when a specified route was learnt, in seconds.

PIM Commands

This section describes the commands you use to configure Protocol Independent Multicast -Dense Mode (PIM-DM) and Protocol Independent Multicast - Sparse Mode (PIM-SM). PIM-DM and PIM-SM are multicast routing protocols that provides scalable inter-domain multicast routing across the Internet, independent of the mechanisms provided by any particular unicast routing protocol. Only one PIM mode can be operational at a time.

ip pim dense

This command enables the administrative mode of PIM-DM in the router.

Default disabled

Format `ip pim dense`

Mode Global Config

no ip pim dense

This command disables the administrative mode of PIM-DM in the router.

Format `no ip pim dense`

Mode Global Config

ip pim sparse

This command enables the administrative mode of PIM-SM in the router.

Default disabled

Format `ip pim sparse`

Mode Global Config

no ip pim sparse

This command disables the administrative mode of PIM-SM in the router.

Format `no ip pim sparse`

Mode Global Config

ip pim

This command administratively enables PIM on an interface or range of interfaces.

Default disabled

Format `ip pim`

Mode Interface Config

no ip pim

This command sets the administrative mode of PIM on an interface to disabled.

Format `no ip pim`

Mode Interface Config

ip pim hello-interval

This command configures the transmission frequency of hello messages the interface or range of interfaces sends to PIM-enabled neighbors. This field has a range of 10 to 18000 seconds.

Default 30

Format `ip pim hello-interval` *seconds*

Mode Interface Config

no ip pim hello-interval

This command resets the transmission frequency of hello messages between PIM enabled neighbors to the default value.

Format `no ip pim hello-interval`

Mode Interface Config

ip pim bsr-border

Use this command to prevent bootstrap router (BSR) messages from being sent or received through an interface or range of interfaces.

Note: This command takes effect only when PIM-SM is configured as the PIM mode.

Default disabled

Format `ip pim bsr-border`

Mode Interface Config

no ip pim bsr-border

Use this command to disable the interface from being the BSR border.

Format `no ip pim bsr-border`

Mode Interface Config

ip pim bsr-candidate

This command is used to configure the router to announce its candidacy as a bootstrap router (BSR).

Note: This command takes effect only when PIM-SM is configured as the PIM mode.

Default None

Format `ip pim bsr-candidate interface slot/port` *`hash-mask-length [priority]`*

Mode Global Config

Parameters	*Description*
hash-mask-length	Length of a mask (32 bits maximum) that is to be ANDed with the group address before the hash function is called. All groups with the same seed hash correspond to the same RP. For example, if this value was 24, only the first 24 bits of the group addresses matter. This allows you to get one RP for multiple groups.
priority	Priority of the candidate BSR. The range is an integer from 0 to 255. The BSR with the larger priority is preferred. If the priority values are the same, the router with the larger IP address is the BSR. The default value is 0.

no ip pim bsr-candidate

This command is used to disable the router to announce its candidacy as a bootstrap router (BSR).

Format `no ip pim bsr-candidate interface slot/port` *`hash-mask-length [priority]`*

Mode Global Config

ip pim dr-priority

Use this command to set the priority value for which a router is elected as the designated router (DR). This command can be configured on a single interface or a range of interfaces.

Note: This command takes effect only when PIM-SM is configured as the PIM mode.

Default 1

Format `ip pim dr-priority` *`0-2147483647`*

Mode Interface Config

no ip pim dr-priority

Use this command to disable the interface from being the BSR border.

Format `no ip pim dr-priority`

Mode Interface Config

ip pim join-prune-interval

This command is used to configure the join/prune interval for the PIM-SM router on an interface or range of interfaces. The join/prune interval is specified in seconds. This parameter can be configured to a value from 0 to 18000.

Note: This command takes effect only when PIM-SM is configured as the PIM mode.

Default 60

Format `ip pim join-prune-interval` *`0-18000`*

Mode Interface Config

no ip pim join-prune-interval

Use this command to set the join/prune interval to the default value.

Format `no ip pim join-prune-interval`

Mode Interface Config

ip pim register-rate-limit

This command sets a limit on the maximum number of PIM-SM register messages sent, in kilobits per second, for each (S,G) entry. The valid values are from (0 to 2000 kilobits/sec).

Note: This command takes effect only when PIM-SM is configured as the PIM mode.

Default 0

Format `ip pim register-rate-limit` *`0-2000`*

Mode Global Config

no ip pim register-rate-limit

This command resets the register rate limit to the default value.

Format `no ip pim register-rate-limit`

Mode Global Config

ip pim rp-address

This command is used to statically configure the RP address for one or more multicast groups. The parameter *rp-address* 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. The optional keyword override indicates that if there is a conflict, the RP configured with this command prevails over the RP learned by BSR.

Note: This command takes effect only when PIM-SM is configured as the PIM mode.

Default 0

Format `ip pim rp-address rp-address group-address group-mask [override]`

Mode Global Config

no ip pim rp-address

This command is used to statically remove the RP address for one or more multicast groups.

Format `no ip pim rp-address rp-address group-address group-mask`

Mode Global Config

ip pim rp-candidate

This command is used to configure the router to advertise itself as a PIM candidate rendezvous point (RP) to the bootstrap router (BSR).

Note: This command takes effect only when PIM-SM is configured as the PIM mode.

Default None

Format `ip pim rp-candidate interface slot/port group-address group-mask`

Mode Global Config

no ip pim rp-candidate

This command is used to disable the router to advertise itself as a PIM candidate rendezvous point (RP) to the bootstrap router (BSR).

Format `no ip pim rp-candidate interface slot/port group-address group-mask`

Mode Global Config

ip pim spt-threshold

Use this command to configure the Data Threshold rate for the last-hop router to switch to the shortest path. The rate is specified in Kilobits per second. The possible values are 1 to 2000.

Note: Some DWS-4000 platforms do not support a non-zero data threshold rate. For these platforms, only a *Switch on First Packet* policy is supported.

Note: This command takes effect only when PIM-SM is configured as the PIM mode.

Default 0

Format `ip pim spt-threshold 1-2000`

Mode Global Config

no ip pim spt-threshold

This command is used to set the Data Threshold rate for the RP router to the default value.

Format `no ip pim spt-threshold`

Mode Global Config

ip pim ssm

Use this command to define the Source Specific Multicast (SSM) range of IP multicast addresses.

Note: This command takes effect only when PIM-SM is configured as the PIM mode.

Default disabled

Format `ip pim ssm {default | group-address group-mask}`

Mode Global Config

Parameter	*Description*
default-range	Defines the SSM range access list to 232/8.

no ip pim ssm

This command is used to disable the Source Specific Multicast (SSM) range.

Format `no ip pim ssm`

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

show ip pim

This command displays the system-wide information for PIM-DM or PIM-SM.

Format `show ip pim`

Modes
- Privileged EXEC
- User EXEC

Note: If the PIM mode is PIM-DM (dense), some of the fields in the following table do not display in the command output because they are applicable only to PIM-SM.

Term	*Definition*
PIM Mode	Indicates whether the PIM mode is dense (PIM-DM) or sparse (PIM-SM)
Data Threshold Rate	Rate (in kbps) of SPT Threshold
Register Rate-limit	Rate (in kbps) of the Register Threshold
Interface	*slot/port*
Interface Mode	Indicates whether PIM is enabled or disabled on this interface.
Operational Status	The current state of PIM on this interface: Operational or Non-Operational.

show ip pim ssm

This command displays the configured source specific IP multicast addresses. If no SSM Group range is configured, this command output is `No SSM address range is configured`.

Format `show ip pim ssm`

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
Group Address	The IP multicast address of the SSM group.
Prefix Length	The network prefix length.

show ip pim interface

This command displays the interface information for PIM on the specified interface. If no interface is specified, the command displays the status parameters for all PIM-enabled interfaces.

Format `show ip pim interface [slot/port]`

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
Interface	*slot/port*
Mode	Indicates whether the PIM mode enabled on the interface is dense or sparse.
Hello Interval	The frequency at which PIM hello messages are transmitted on this interface. By default, the value is 30 seconds.
Join Prune Interval	The join/prune interval for the PIM router. The interval is in seconds.
DR Priority	The priority of the Designated Router configured on the interface. This field is not applicable if the interface mode is Dense
BSR Border	Identifies whether this interface is configured as a bootstrap router border interface.
Neighbor Count	The number of PIM neighbors learned on this interface. This is a dynamic value and is shown only when a PIM interface is operational.
Designated Router	The IP address of the elected Designated Router for this interface. This is a dynamic value and will only be shown when a PIM interface is operational. This field is not applicable if the interface mode is Dense

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

```
(switch) #show ip pim interface

Interface.....................................1/0/1
  Mode........................................Sparse
  Hello Interval (secs).......................30
  Join Prune Interval (secs)..................60
```

```
  DR Priority.....................................1
  BSR Border......................................Disabled
  Neighbor Count..................................1
  Designated Router...............................192.168.10.1

(switch) #show ip pim interface

Interface.......................................1/0/1
  Mode..........................................Dense
  Hello Interval (secs)...........................30
  Join Prune Interval (secs)......................60
  DR Priority.....................................NA
  BSR Border......................................Disabled
  Neighbor Count..................................1
  Designated Router...............................NA
```

If none of the interfaces are enabled for PIM, the following message is displayed:

```
None of the routing interfaces are enabled for PIM.
```

show ip pim neighbor

This command displays PIM neighbors discovered by PIMv2 Hello messages. If the interface number is not specified, this command displays the neighbors discovered on all the PIM enabled interfaces.

Format `show ip pim neighbor [slot/port]`

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
Neighbor Address	The IP address of the neighbor on an interface.
Interface	*slot/port*
Up Time	The time since this neighbor has become active on this interface.
Expiry Time	The expiry time of the neighbor on this interface.
DR Priority	The DR Priority configured on this Interface (PIM-SM only). ***Note:*** DR Priority is applicable only when sparse-mode configured routers are neighbors. Otherwise, NA is displayed in this field.

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

```
(switch) #show ip pim neighbor 1/0/1

Neighbor Addr   Interface Uptime      Expiry Time DR
                          (hh:mm:ss) (hh:mm:ss)   Priority
--------------- --------- ----------- ----------- --------
192.168.10.2    1/0/1     00:02:55     00:01:15   NA


(switch) #show ip pim neighbor

Neighbor Addr   Interface  Uptime      Expiry Time DR
                           (hh:mm:ss) (hh:mm:ss)   Priority
--------------- ---------  ----------- ----------- --------
```

```
192.168.10.2    1/0/1      00:02:55     00:01:15   1
192.168.20.2    1/0/2      00:03:50     00:02:10   1
```

If no neighbors have been learned on any of the interfaces, the following message is displayed:

```
No neighbors exist on the router.
```

show ip pim bsr-router

This command displays the bootstrap router (BSR) information.

Format `show ip pim bsr-router {candidate | elected}`

Mode
- Privileged EXEC
- User EXEC

Term	*Definition*
BSR Address	IP address of the BSR.
BSR Priority	Priority as configured in the `ip pim bsr-candidate` command.
BSR Hash Mask Length	Length of a mask (maximum 32 bits) that is to be ANDed with the group address before the hash function is called. This value is configured in the `ip pim bsr-candidate` command.
Next Bootstrap Message	Time (in hours, minutes, and seconds) in which the next bootstrap message is due from this BSR.
Next Candidate RP advertisement	Time (in hours, minutes, and seconds) in which the next candidate RP advertisement will be sent.

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

```
(switch) #show ip pim bsr-router candidate

BSR Address.....................................192.168.10.1
  BSR Priority.....................................0
  BSR Hash Mask Length.............................32
  Next Bootstrap message (hh:mm:ss).....................NA
  Next Candidate RP Advertisement (hh:mm:ss).............NA

(switch) #show ip pim bsr-router elected

BSR Address.....................................192.168.10.1
  BSR Priority.....................................0
  BSR Hash Mask Length.............................32
  Next Bootstrap message (hh:mm:ss).....................00:00:05
  Next Candidate RP Advertisement (hh:mm:ss).............00:00:02
```

If no configured or elected BSRs exist on the router, the following message is displayed:

```
No BSR's exist/learned on this router.
```

show ip pim rp-hash

This command displays which rendezvous point (RP) is being used for a specified group.

Format `show ip pim rp-hash group-address`

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
RP Address	The IP address of the RP for the group specified.
Type	Indicates the mechanism (BSR or static) by which the RP was selected.

show ip pim rp mapping

Use this command to display all active group-to-RP mappings of which the router is a aware (either configured or learned from the bootstrap router (BSR)). Use the optional parameters to limit the display to a specific RP address or to view group-to-candidate RP or group to Static RP mapping information.

Format `show ip pim rp mapping [{rp-address | candidate | static}]`

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
RP Address	The IP address of the RP for the group specified.
Group Address	The IP address of the multicast group.
Group Mask	The subnet mask associated with the group.
Origin	Indicates the mechanism (BSR or static) by which the RP was selected.
Expiry Time	The expiry time of the RP mapping.

Internet Group Message Protocol Commands

This section describes the commands you use to view and configure Internet Group Message Protocol (IGMP) settings.

ip igmp

This command sets the administrative mode of IGMP in the system to active on an interface, range of interfaces, or on all interfaces.

Default disabled

Format `ip igmp`

Modes
- Global Config
- Interface Config

no ip igmp

This command sets the administrative mode of IGMP in the system to inactive.

Format `no ip igmp`

Modes
- Global Config
- Interface Config

ip igmp version

This command configures the version of IGMP for an interface or range of interfaces. The value for *version* is either 1, 2 or 3.

Default 3

Format `ip igmp version` *version*

Modes Interface Config

no ip igmp version

This command resets the version of IGMP to the default value.

Format `no ip igmp version`

Modes Interface Config

ip igmp last-member-query-count

This command sets the number of Group-Specific Queries sent by the interface or range of interfaces 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*

Modes 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`

Modes 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. This value can be configured on one interface or a range of interfaces

Default 10 tenths of a second (1 second)

Format `ip igmp last-member-query-interval` *seconds*

Modes 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`

Modes Interface Config

ip igmp query-interval

This command configures the query interval for the specified interface or range of interfaces. The query interval determines how fast IGMP Host-Query packets are transmitted on this interface. The range for `query-interval` is 1 to 3600 seconds.

Default 125 seconds

Format `ip igmp query-interval` *seconds*

Modes 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`

Modes Interface Config

ip igmp query-max-response-time

This command configures the maximum response time interval for the specified interface or range of interfaces, 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 `igmp query-max-response-time` is 0 to 255 tenths of a second.

Default 100

Format `ip igmp query-max-response-time 0-255`

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 or range of interfaces. 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 1-255`

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 or range of interfaces. The range for *count* is 1 to 20.

Default 2

Format `ip igmp startup-query-count 1-20`

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 or range of interfaces. The time interval value is in seconds. The range for *`interval`* is 1 to 300 seconds.

Default 31

Format `ip igmp startup-query-interval` *`1-300`*

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

Term	*Definition*
IGMP Admin Mode	The administrative status of IGMP. This is a configured value.
Interface	*slot/port*
Interface Mode	Indicates whether IGMP is enabled or disabled on the interface. This is a configured value.
Protocol State	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

If you do not use the detail keyword, the following fields appear:

Term	*Definition*
IP Address	The IP address of the interface participating in the multicast group.
Subnet Mask	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:

Term	*Definition*
Querier Status	This displays whether the interface has IGMP in Querier mode or Non-Querier mode.
Groups	The list of multicast groups that are registered on this interface.

If you use the detail keyword, the following fields appear:

Term	*Definition*
Multicast IP Address	The IP address of the registered multicast group on this interface.
Last Reporter	The IP address of the source of the last membership report received for the specified multicast group address on this interface.
Up Time	The time elapsed since the entry was created for the specified multicast group address on this interface.
Expiry Time	The amount of time remaining to remove this entry before it is aged out.
Version1 Host Timer	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	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

Term	*Definition*
Interface	*slot/port*
IGMP Admin Mode	The administrative status of IGMP.
Interface Mode	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

Term	*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:

Term	*Definition*
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

Term	*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 an interface or range of interfaces. To enable the IGMP Proxy on an interface, 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 interface or range of interfaces. This command is valid only when you enable IGMP Proxy on the interface or range of interfaces. The value of *interval* can be 1–260 seconds.

Default 1

Format `ip igmp-proxy unsolicit-rprt-interval` *1-260*

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 interface (or range of interfaces). 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`

Modes
- Privileged EXEC
- User EXEC

Term	*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.
Number of Multicast Groups	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.

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

```
(Routing) #show ip igmp-proxy

Interface Index..................................... 1/0/1
Admin Mode.......................................... Enable
Operational Mode.................................... Enable
Version............................................. 3
Num of Multicast Groups..... 0
Unsolicited Report Interval..... 1
Querier IP Address on Proxy Interface..... 5.5.5.50
Older Version 1 Querier Timeout..... 0
Older Version 2 Querier Timeout..... 00::00:00
Proxy Start Frequency..... 1
```

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`

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
Interface Index	The slot/port of the IGMP proxy.

The column headings of the table associated with the interface are as follows:

Term	*Definition*
Ver	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. Valid for version 2 only.
Leaves Sent	Number of IGMP leaves sent on the Proxy interface. Valid for version 2 only.

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

```
(Routing) #show ip igmp-proxy interface

Interface Index.............................. 1/0/1

Ver  Query Rcvd  Report Rcvd  Report Sent  Leave Rcvd  Leave Sent
-----------------------------------------------------------------
1      0             0             0          -----          -----
2      0             0             0           0              0
3      0             0             0          -----          -----
```

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`

Modes
- Privileged EXEC
- User EXEC

Term	*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.

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

```
(Routing) #show ip igmp-proxy groups

Interface Index.............................. 1/0/1

Group Address    Last Reporter    Up Time   Member State  Filter Mode  Sources
-------------     -------------- ---------- ------------- ------------- -------
225.4.4.4         5.5.5.48          00:02:21  DELAY_MEMBER       Include        3

226.4.4.4         5.5.5.48          00:02:21  DELAY_MEMBER       Include        3

227.4.4.4         5.5.5.48          00:02:21  DELAY_MEMBER       Exclude        0

228.4.4.4         5.5.5.48          00:02:21  DELAY_MEMBER       Include        3
```

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`

Modes
- Privileged EXEC
- User EXEC

Term	*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.

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

```
(Routing) #show ip igmp-proxy groups

Interface Index.............................. 1/0/1

Group Address    Last Reporter    Up Time   Member State Filter Mode  Sources
-------------     -------------- ----------- ------------ ------------ ---------
225.4.4.4         5.5.5.48          00:02:21  DELAY_MEMBER       Include         3

Group Source List             Expiry Time
-----------------             -----------------
5.1.2.3                          00:02:21
6.1.2.3                          00:02:21
7.1.2.3                          00:02:21

226.4.4.4         5.5.5.48          00:02:21  DELAY_MEMBER       Include         3

Group Source List             Expiry Time
------------------            ---------------
2.1.2.3                          00:02:21
6.1.2.3                          00:01:44
8.1.2.3                          00:01:44
```

```
227.4.4.4          5.5.5.48          00:02:21  DELAY_MEMBER       Exclude        0


228.4.4.4          5.5.5.48          00:03:21  DELAY_MEMBER       Include         3

Group Source List             Expiry Time
------------------            ---------------
9.1.2.3                          00:03:21
6.1.2.3                          00:03:21
7.1.2.3                          00:03:21
```

Section 11: IPv6 Multicast Commands

This chapter describes the IPv6 Multicast commands available in the DWS-4000 CLI.

Note: There is no specific IP multicast enable for IPv6. Enabling of multicast at global config is common for both IPv4 and IPv6.

This chapter contains the following sections:

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

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

IPv6 Multicast Forwarder

show ipv6 mroute

Note: There is no specific IP multicast enable for IPv6. Enabling of multicast at global config is common for both IPv4 and IPv6.

Use this command to show the mroute entries specific for IPv6. (This command is the IPv6 equivalent of the IPv4 `show ip mcast mroute` command.)

Format `show ipv6 mroute {[detail] | [summary] | [group {group-address} [detail | summary]] | [source {source-address} [grpaddr | summary ]]}`

Modes
- Privileged EXEC
- User EXEC

If you use the *detail* parameter, the command displays the following Multicast Route Table fields:

Term	*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:

Term	*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 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 ipv6 mroute group

This command displays the multicast configuration settings specific to IPv6 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 group IPv6 address *group-address*.

Format `show ipv6 mroute group group-address {detail | summary}`

Modes
- Privileged EXEC
- User EXEC

Term	*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 ipv6 mroute source

This command displays the multicast configuration settings specific to IPv6 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 ipv6 mroute source source-address {grpaddr | summary}`

Modes
- Privileged EXEC
- User EXEC

If you use the *groupipaddr* parameter, the command displays the following column headings in the output table:

Term	*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:

Term	*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.

IPv6 PIM Commands

This section describes the commands you use to configure Protocol Independent Multicast -Dense Mode (PIM-DM) and Protocol Independent Multicast - Sparse Mode (PIM-SM) for IPv6 multicast routing. PIM-DM and PIM-SM are multicast routing protocols that provides scalable inter-domain multicast routing across the Internet, independent of the mechanisms provided by any particular unicast routing protocol. Only one PIM mode can be operational at a time.

ipv6 pim dense

This command enables the administrative mode of PIM-DM in the router.

Default disabled

Format `ipv6 pim dense`

Mode Global Config

no ipv6 pim dense

This command disables the administrative mode of PIM-DM in the router.

Format `no ipv6 pim dense`

Mode Global Config

ipv6 pim sparse

This command enables the administrative mode of PIM-SM in the router.

Default disabled

Format `ipv6 pim sparse`

Mode Global Config

no ipv6 pim sparse

This command disables the administrative mode of PIM-SM in the router.

Format `no ipv6 pim sparse`

Mode Global Config

ipv6 pim

This command administratively enables PIM on an interface or range of interfaces.

Default disabled

Format `ipv6 pim`

Mode Interface Config

no ipv6 pim

This command sets the administrative mode of PIM on an interface to disabled.

Format `no ipv6 pim`

Mode Interface Config

ipv6 pim hello-interval

Use this command to configure the PIM hello interval for the specified router interface or range of interfaces. The hello-interval is specified in seconds and is in the range 0–18000.

Default 30

Format `ipv6 pim hello-interval` *`0–18000`*

Mode Interface Config

no ipv6 pim hello-interval

Use this command to set the PIM hello interval to the default value.

Format `no ipv6 pim hello-interval`

Mode Interface Config

ipv6 pim bsr-border

Use this command to prevent bootstrap router (BSR) messages from being sent or received through an interface or range of interfaces.

Note: This command takes effect only when PIM-SM is configured as the PIM mode.

Default disabled

Format `ipv6 pim bsr-border`

Mode Interface Config

no ipv6 pim bsr-border

Use this command to disable the interface from being the BSR border.

Format `no ipv6 pim bsr-border`

Mode Interface Config

ipv6 pim bsr-candidate

This command is used to configure the router to announce its candidacy as a bootstrap router (BSR).

Note: This command takes effect only when PIM-SM is configured as the PIM mode.

Default None

Format `ipv6 pim bsr-candidate interface slot/port` *`hash-mask-length [priority]`*

Mode Global Config

Parameters	*Description*
hash-mask-length	Length of a mask (32 bits maximum) that is to be ANDed with the group address before the hash function is called. All groups with the same seed hash correspond to the same RP. For example, if this value was 24, only the first 24 bits of the group addresses matter. This allows you to get one RP for multiple groups.
priority	Priority of the candidate BSR. The range is an integer from 0 to 255. The BSR with the larger priority is preferred. If the priority values are the same, the router with the larger IPv6 address is the BSR. The default value is 0.

no ipv6 pim bsr-candidate

This command is used to disable the router to announce its candidacy as a bootstrap router (BSR).

Format `no ipv6 pim bsr-candidate interface slot/port` *`hash-mask-length [priority]`*

Mode Global Config

ipv6 pim dr-priority

Use this command to set the priority value for which a router is elected as the designated router (DR). This command can be configured on a single interface or a range of interfaces.

Note: This command takes effect only when PIM-SM is configured as the PIM mode.

Default 1

Format `ipv6 pim dr-priority` *`0-2147483647`*

Mode Interface Config

no ipv6 pim dr-priority

Use this command to disable the interface from being the BSR border.

Format `no ipv6 pim dr-priority`

Mode Interface Config

ipv6 pim join-prune-interval

This command is used to configure the join/prune interval for the PIM-SM router on an interface or range of interfaces. The join/prune interval is specified in seconds. This parameter can be configured to a value from 0 to 18000.

Note: This command takes effect only when PIM-SM is configured as the PIM mode.

Default 60

Format `ipv6 pim join-prune-interval` *`0-18000`*

Mode Interface Config

no ipv6 pim join-prune-interval

Use this command to set the join/prune interval to the default value.

Format `no ipv6 pim join-prune-interval`

Mode Interface Config

ipv6 pim register-rate-limit

This command sets a limit on the maximum number of PIM-SM register messages sent, in kilobits per second, for each (S,G) entry. The valid values are from (0 to 2000 kilobits/sec).

Note: This command takes effect only when PIM-SM is configured as the PIM mode.

Default 0

Format `ipv6 pim register-rate-limit` *`0-2000`*

Mode Global Config

no ipv6 pim register-rate-limit

This command resets the register rate limit to the default value.

Format `no ipv6 pim register-rate-limit`

Mode Global Config

ipv6 pim rp-address

This command is used to statically configure the RP address for one or more multicast groups. The parameter *`rp-address`* is the IPv6 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. The optional keyword `override` indicates that if there is a conflict, the RP configured with this command prevails over the RP learned by BSR.

Note: This command takes effect only when PIM-SM is configured as the PIM mode.

Default 0

Format `ipv6 pim rp-address` *`rp-address group-address/prefix-length`* `[override]`

Mode Global Config

no ipv6 pim rp-address

This command is used to statically remove the RP address for one or more multicast groups.

Format `no ipv6 pim rp-address` *`rp-address group-address/prefix-length`*

Mode Global Config

ipv6 pim rp-candidate

This command is used to configure the router to advertise itself as a PIM candidate rendezvous point (RP) to the bootstrap router (BSR).

Note: This command takes effect only when PIM-SM is configured as the PIM mode.

Default None

Format `ipv6 pim rp-candidate interface slot/port` *`group-address/prefix-length`*

Mode Global Config

no ipv6 pim rp-candidate

This command is used to disable the router to advertise itself as a PIM candidate rendezvous point (RP) to the bootstrap router (BSR).

Format `no ipv6 pim rp-candidate interface slot/port` *`group-address/prefix-length`*

Mode Global Config

ipv6 pim spt-threshold

Use this command to configure the Data Threshold rate for the last-hop router to switch to the shortest path. The rate is specified in Kilobits per second. The possible values are 1 to 2000.

Note: Some DWS-4000 platforms do not support a non-zero data threshold rate. For these platforms, only a *Switch on First Packet* policy is supported.

Note: This command takes effect only when PIM-SM is configured as the PIM mode.

Default 0

Format `ipv6 pim spt-threshold` *`1-2000`*

Mode Global Config

no ipv6 pim spt-threshold

This command is used to set the Data Threshold rate for the RP router to the default value.

Format `no ipv6 pim spt-threshold`

Mode Global Config

ipv6 pim ssm

Use this command to define the Source Specific Multicast (SSM) range of IPv6 multicast addresses.

Note: Some DWS-4000 platforms do not support a non-zero data threshold rate. For these platforms, only a *Switch on First Packet* policy is supported.

Default disabled

Format `ipv6 pim ssm {default | group-address/prefix-length}`

Mode Global Config

Parameter	*Description*
default-range	Defines the SSM range access list FF3x::/32.

no ipv6 pim ssm

This command is used to disable the specified Source Specific Multicast (SSM) range.

Format `no ipv6 pim ssm {default | group-address/prefix-length}`

Mode Global Config

ipv6 pim-trapflags

This command enables the PIM trap mode for both Sparse Mode (SM) and Dense Mode. (DM).

Default disabled

Format `ipv6 pim-trapflags`

Mode Global Config

no ipv6 pim-trapflags

This command sets the PIM trap mode to the default.

Format `no ipv6 pim-trapflags`

Mode Global Config

show ipv6 pim

This command displays the system-wide information for PIM-DM or PIM-SM.

Format `show ipv6 pim`

Modes
- Privileged EXEC
- User EXEC

Note: If the PIM mode is PIM-DM (dense), some of the fields in the following table do not display in the command output because they are applicable only to PIM-SM.

Term	*Definition*
PIM Mode	Indicates whether the PIM mode is dense (PIM-DM) or sparse (PIM-SM)
Data Threshold Rate	Rate (in kbps) of SPT Threshold
Register Rate-limit	Rate (in kbps) of the Register Threshold
Interface	*slot/port*
Interface Mode	Indicates whether PIM is enabled or disabled on this interface.
Operational Status	The current state of PIM on this interface: Operational or Non-Operational.

show ipv6 pim ssm

This command displays the configured source specific IPv6 multicast addresses. If no SSM Group range is configured, this command output is `No SSM address range is configured`.

Format `show ipv6 pim ssm`

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
Group Address	The IPv6 multicast address of the SSM group.
Prefix Length	The network prefix length.

show ipv6 pim interface

This command displays the interface information for PIM on the specified interface. If no interface is specified, the command displays the status parameters for all PIM-enabled interfaces.

Format `show ipv6 pim interface [slot/port]`

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
Interface	*slot/port*
Mode	Indicates whether the PIM mode enabled on the interface is dense or sparse.
Hello Interval	The frequency at which PIM hello messages are transmitted on this interface. By default, the value is 30 seconds.
Join Prune Interval	The join/prune interval for the PIM router. The interval is in seconds.
DR Priority	The priority of the Designated Router configured on the interface. This field is not applicable if the interface mode is Dense
BSR Border	Identifies whether this interface is configured as a bootstrap router border interface.
Neighbor Count	The number of PIM neighbors learned on this interface. This is a dynamic value and is shown only when a PIM interface is operational.
Designated Router	The IP address of the elected Designated Router for this interface. This is a dynamic value and will only be shown when a PIM interface is operational. This field is not applicable if the interface mode is Dense

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

```
(switch) #show ipv6 pim interface

Interface.....................................1/0/1
  Mode........................................Sparse
  Hello Interval (secs).......................30
  Join Prune Interval (secs)..................60
  DR Priority.................................1
  BSR Border..................................Disabled
  Neighbor Count..............................1
  Designated Router...........................2001:DB8:52::/32

(switch) #show ipv6 pim interface

Interface.....................................1/0/1
  Mode........................................Dense
  Hello Interval (secs).......................30
  Join Prune Interval (secs)..................60
  DR Priority.................................NA
  BSR Border..................................Disabled
  Neighbor Count..............................1
  Designated Router...........................NA
```

If none of the interfaces are enabled for PIM, the following message is displayed:

```
None of the routing interfaces are enabled for PIM.
```

show ipv6 pim neighbor

This command displays PIM neighbors discovered by PIMv2 Hello messages. If the interface number is not specified, this command displays the neighbors discovered on all the PIM enabled interfaces.

Format `show ipv6 pim neighbor [slot/port]`

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
Neighbor Address	The IPv6 address of the neighbor on an interface.
Interface	*slot/port*
Up Time	The time since this neighbor has become active on this interface.
Expiry Time	The expiry time of the neighbor on this interface.

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

```
(switch) #show ipv6 pim neighbor

Neighbor Addr      Interface  Uptime      Expiry Time
                             (HH:MM::SS) (HH:MM::SS)
---------------    ---------  ----------- -----------
2001:DB8:39::/32   1/0/1      00:02:55    00:01:15
2001:DB8:A3::/32   1/0/2      00:03:50    00:02:10
```

If no neighbors have been learned on any of the interfaces, the following message is displayed:

```
No neighbors are learnt on any interface.
```

show ipv6 pim bsr-router

This command displays the bootstrap router (BSR) information.

Format `show ipv6 pim bsr-router {candidate | elected}`

Mode
- Privileged EXEC
- User EXEC

Term	*Definition*
BSR Address	IPv6 address of the BSR.
BSR Priority	Priority as configured in the `ipv6 pim bsr-candidate` command.
BSR Hash Mask Length	Length of a mask (maximum 32 bits) that is to be ANDed with the group address before the hash function is called. This value is configured in the `ipv6 pim bsr-candidate` command.
Next Bootstrap Message	Time (in hours, minutes, and seconds) in which the next bootstrap message is due from this BSR.
Next Candidate RP advertisement	Time (in hours, minutes, and seconds) in which the next candidate RP advertisement will be sent.

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

```
(switch) #show ipv6 pim bsr-router candidate

BSR Address.....................................2001:DB8:8C2::/32
  BSR Priority.....................................0
  BSR Hash Mask Length.............................32
  Next Bootstrap message (hh:mm:ss).....................NA
  Next Candidate RP Advertisement (hh:mm:ss).............NA

(switch) #show ipv6 pim bsr-router elected

BSR Address.....................................2001:DB8:8C2::/32
  BSR Priority.....................................0
  BSR Hash Mask Length.............................32
  Next Bootstrap message (hh:mm:ss).....................00:00:05
  Next Candidate RP Advertisement (hh:mm:ss).............00:00:02
```

If no configured or elected BSRs exist on the router, the following message is displayed:

```
No BSR's exist/learned on this router.
```

show ipv6 pim rp-hash

This command displays which rendezvous point (RP) is being used for a specified group.

Format `show ipv6 pim rp-hash` *`group-address`*

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
RP Address	The IPv6 address of the RP for the group specified.
Type	Indicates the mechanism (BSR or static) by which the RP was selected.

show ipv6 pim rp mapping

Use this command to display all active group-to-RP mappings of which the router is a aware (either configured or learned from the bootstrap router (BSR)). Use the optional parameters to limit the display to a specific RP address or to view group-to-candidate RP or group to Static RP mapping information.

.

Format `show ipv6 pim rp mapping [{`*`rp-address`*` | candidate | static}]`

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
RP Address	The IPv6 address of the RP for the group specified.
Group Address	The IPv6 address and prefix length of the multicast group.
Origin	Indicates the mechanism (BSR or static) by which the RP was selected.
Expiry Time	The expiry time of the RP mapping.

IPv6 MLD Commands

IGMP/MLD Snooping is Layer 2 functionality but IGMP/MLD are Layer 3 multicast protocols. It requires that in a network setup there should be a multicast router (which can act as a querier) to be present to solicit the multicast group registrations. However some network setup does not need a multicast router as multicast traffic is destined to hosts within the same network. In this situation, DWS-4000 has an IGMP/MLD Snooping Querier running on one of the switches and Snooping enabled on all the switches. For more information, see "IGMP Snooping Configuration Commands" on page 344 and "MLD Snooping Commands" on page 354.

ipv6 mld router

Use this command, in the administrative mode of the router, to enable MLD in the router.

Default	Disabled
Format	`ipv6 mld router`
Mode	Global Config

no ipv6 mld router

Use this command, in the administrative mode of the router, to disable MLD in the router.

Default	Disabled
Format	`no ipv6 mld router`
Mode	Global Config

ipv6 mld query-interval

Use this command to set the MLD router's query interval for the interface or range of interfaces. The query-interval is the amount of time between the general queries sent when the router is the querier on that interface. The range for *`query-interval`* is 1 to 3600 seconds.

Default	125
Format	`ipv6 mld query-interval` *`query-interval`*
Mode	Interface Config

no ipv6 mld query-interval

Use this command to reset the MLD query interval to the default value for that interface.

Format	`no ipv6 mld query-interval`
Mode	Interface Config

ipv6 mld query-max-response-time

Use this command to set the MLD querier's maximum response time for the interface or range of interfaces and this value is used in assigning the maximum response time in the query messages that are sent on that interface. The range for *query-max-response-time* is 0 to 65535 milliseconds.

Default 10000 milliseconds

Format `ipv6 mld query-max-response-time` *query-max-response-time*

Mode Interface Config

no ipv6 mld query-max-response-time

This command resets the MLD query max response time for the interface to the default value.

Format `no ipv6 mld query-max-response-time`

Mode Interface Config

ipv6 mld last-member-query-interval

Use this command to set the last member query interval for an MLD interface or range of interfaces, which is the value of the maximum response time parameter in the group specific queries sent out of this interface. The range for *last-member-query-interval* is 0 to 65535 milliseconds.

Default 1000 milliseconds

Format `ipv6 mld last-member-query-interval` *last-member-query-interval*

Mode Interface Config

no ipv6 mld last-member-query-interval

Use this command to reset the *last-member-query-interval* parameter of the interface to the default value.

Format `no ipv6 mld last-member-query-interval`

Mode Interface Config

ipv6 mld last-member-query-count

Use this command to set the number of listener-specific queries sent before the router assumes that there are no local members on an interface or range of interfaces. The range for *last-member-query-count* is 1 to 20.

Default 2

Format `ipv6 mld last-member-query-count` *last-member-query-count*

Mode Interface Config

no ipv6 mld last-member-query-count

Use this command to reset the *last-member-query-count* parameter of the interface to the default value.

Format `no ipv6 mld last-member-query-count`

Mode Interface Config

show ipv6 mld groups

Use this command to display information about multicast groups that MLD reported. The information is displayed only when MLD is enabled on at least one interface. If MLD was not enabled on even one interface, there is no group information to be displayed.

Format `show ipv6 mld groups {slot/port | group-address}`

Mode
- Privileged EXEC
- User EXEC

The following fields are displayed as a table when slot/port is specified.

Field	*Description*
Group Address	The address of the multicast group.
Interface	Interface through which the multicast group is reachable.
Up Time	Time elapsed in hours, minutes, and seconds since the multicast group has been known.
Expiry Time	Time left in hours, minutes, and seconds before the entry is removed from the MLD membership table.

When *group-address* is specified, the following fields are displayed for each multicast group and each interface.

Field	*Description*
Interface	Interface through which the multicast group is reachable.
Group Address	The address of the multicast group.

Field	*Description*
Last Reporter	The IP Address of the source of the last membership report received for this multicast group address on that interface.
Filter Mode	The filter mode of the multicast group on this interface. The values it can take are *include* and *exclude*.
Version 1 Host Timer	The time remaining until the router assumes there are no longer any MLD version-1 Hosts on the specified interface.
Group Compat Mode	The compatibility mode of the multicast group on this interface. The values it can take are *MLDv1* and *MLDv2*.

The following table is displayed to indicate all the sources associated with this group.

Field	*Description*
Source Address	The IP address of the source.
Uptime	Time elapsed in hours, minutes, and seconds since the source has been known.
Expiry Time	Time left in hours, minutes, and seconds before the entry is removed.

Example: The following shows examples of CLI display output for the commands.

```
(Routing) #show ipv6 mld groups ?

group-address           Enter Group Address Info.
<unit/slot/port>          Enter interface in unit/slot/port format.


(Routing) #show ipv6 mld groups 1/0/1

Group Address................................. FF43::3
Interface..................................... 1/0/1
Up Time (hh:mm:ss)............................ 00:03:04
Expiry Time (hh:mm:ss)........................ ------


(Routing) #show ipv6 mld groups ff43::3

Interface..................................... 1/0/1
Group Address................................. FF43::3
Last Reporter................................. FE80::200:FF:FE00:3
Up Time (hh:mm:ss)............................ 00:02:53
Expiry Time (hh:mm:ss)........................ ------
Filter Mode................................... Include
Version1 Host Timer........................... ------
Group compat mode............................. v2
Source Address    ExpiryTime
-----------------  -----------
  2003::10        00:04:17
  2003::20        00:04:17
```

show ipv6 mld interface

Use this command to display MLD-related information for the interface.

Format `show ipv6 mld interface [unit/slot/port]`

Mode
- Privileged EXEC
- User EXEC

The following information is displayed for each of the interfaces or for only the specified interface.

Field	*Description*
Interface	The interface number in slot/port format.
MLD Mode	Displays the configured administrative status of MLD.
Operational Mode	The operational status of MLD on the interface.
MLD Version	Indicates the version of MLD configured on the interface.
Query Interval	Indicates the configured query interval for the interface.
Query Max Response Time	Indicates the configured maximum query response time (in seconds) advertised in MLD queries on this interface.
Robustness	Displays the configured value for the tuning for the expected packet loss on a subnet attached to the interface.
Startup Query interval	This valued indicates the configured interval between General Queries sent by a Querier on startup.
Startup Query Count	This value indicates the configured number of Queries sent out on startup, separated by the Startup Query Interval.
Last Member Query Interval	This value indicates the configured Maximum Response Time inserted into Group-Specific Queries sent in response to Leave Group messages.
Last Member Query Count	This value indicates the configured number of Group-Specific Queries sent before the router assumes that there are no local members.

The following information is displayed if the operational mode of the MLD interface is enabled.

Field	*Description*
Querier Status	This value indicates whether the interface is an MLD querier or non-querier on the subnet it is associated with.
Querier Address	The IP address of the MLD querier on the subnet the interface is associated with.
Querier Up Time	Time elapsed in seconds since the querier state has been updated.
Querier Expiry Time	Time left in seconds before the Querier loses its title as querier.
Wrong Version Queries	Indicates the number of queries received whose MLD version does not match the MLD version of the interface.
Number of Joins	The number of times a group membership has been added on this interface.
Number of Leaves	The number of times a group membership has been removed on this interface.
Number of Groups	The current number of membership entries for this interface.

show ipv6 mld traffic

Use this command to display MLD statistical information for the router.

Format `show ipv6 mld traffic`

Mode
- Privileged EXEC
- User EXEC

Field	*Description*
Valid MLD Packets Received	The number of valid MLD packets received by the router.
Valid MLD Packets Sent	The number of valid MLD packets sent by the router.
Queries Received	The number of valid MLD queries received by the router.
Queries Sent	The number of valid MLD queries sent by the router.
Reports Received	The number of valid MLD reports received by the router.
Reports Sent	The number of valid MLD reports sent by the router.
Leaves Received	The number of valid MLD leaves received by the router.
Leaves Sent	The number of valid MLD leaves sent by the router.
Bad Checksum MLD Packets	The number of bad checksum MLD packets received by the router.
Malformed MLD Packets	The number of malformed MLD packets received by the router.

IPv6 MLD-Proxy Commands

MLD-Proxy is the IPv6 equivalent of IGMP-Proxy. MLD-Proxy commands allow you to configure the network device as well as to view device settings and statistics using either serial interface or telnet session. The operation of MLD-Proxy commands is the same as for IGMP-Proxy: MLD is for IPv6 and IGMP is for IPv4.MGMD is a term used to refer to both IGMP and MLD.

ipv6 mld-proxy

Use this command to enable MLD-Proxy on the interface or range of interfaces. To enable MLD-Proxy on the interface, you must enable multicast forwarding. Also, make sure that there are no other multicast routing protocols enabled n the router.

Format `ipv6 mld-proxy`

Mode Interface Config

no ipv6 mld-proxy

Use this command to disable MLD-Proxy on the router.

Format `no ipv6 mld-proxy`

Mode Interface Config

ipv6 mld-proxy unsolicit-rprt-interval

Use this command to set the unsolicited report interval for the MLD-Proxy interface or range of interfaces. This command is only valid when you enable MLD-Proxy on the interface. The value of *interval* is 1–260 seconds.

Default `1`

Format `ipv6 mld-proxy unsolicit-rprt-interval interval`

Mode Interface Config

no ipv6 mld-proxy unsolicited-report-interval

Use this command to reset the MLD-Proxy router’s unsolicited report interval to the default value.

Format `no ipv6 mld-proxy unsolicit-rprt-interval`

Mode Interface Config

ipv6 mld-proxy reset-status

Use this command to reset the host interface status parameters of the MLD-Proxy interface or range of interfaces. This command is only valid when you enable MLD-Proxy on the interface.

Format `ipv6 mld-proxy reset-status`

Mode Interface Config

show ipv6 mld-proxy

Use this command to display a summary of the host interface status parameters.

Format `show ipv6 mld-proxy`

Mode
- Privileged EXEC
- User EXEC

The command displays the following parameters only when you enable MLD-Proxy.

Field	*Description*
Interface Index	The interface number of the MLD-Proxy.
Admin Mode	Indicates whether MLD-Proxy is enabled or disabled. This is a configured value.
Operational Mode	Indicates whether MLD-Proxy is operationally enabled or disabled. This is a status parameter.
Version	The present MLD host version that is operational on the proxy interface.
Number of Multicast Groups	The number of multicast groups that are associated with the MLD-Proxy interface.
Unsolicited Report Interval	The time interval at which the MLD-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 (MLD-Proxy interface).
Older Version 1 Querier Timeout	The interval used to timeout the older version 1 queriers.
Proxy Start Frequency	The number of times the MLD-Proxy has been stopped and started.

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

```
(Routing) #show ipv6 mld-proxy
Interface Index..................................... 1/0/3
Admin Mode.......................................... Enable
Operational Mode.................................... Enable
Version..................................................... 3
Num of Multicast Groups..................... 0
Unsolicited Report Interval..................... 1
Querier IP Address on Proxy Interface........ fe80::1:2:5
Older Version 1 Querier Timeout.............. 00:00:00
Proxy Start Frequency.....................
```

show ipv6 mld-proxy interface

This command displays a detailed list of the host interface status parameters. It displays the following parameters only when you enable MLD-Proxy.

Format `show ipv6 mld-proxy interface`

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
Interface	The slot/port of the MLD-proxy.

The column headings of the table associated with the interface are as follows:

Term	*Definition*
Ver	The MLD version.
Query Rcvd	Number of MLD queries received.
Report Rcvd	Number of MLD reports received.
Report Sent	Number of MLD reports sent.
Leaves Rcvd	Number of MLD leaves received. Valid for version 2 only.
Leaves Sent	Number of MLD leaves sent on the Proxy interface. Valid for version 2 only.

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

```
(Routing) #show ipv6 mld-proxy interface

Interface Index.............................. 1/0/1

Ver  Query Rcvd  Report Rcvd  Report Sent  Leave Rcvd  Leave Sent
-----------------------------------------------------------------
1      2             0             0             0             2
2      3             0             4          -----         -----
```

show ipv6 mld-proxy groups

Use this command to display information about multicast groups that the MLD-Proxy reported.

Format `show ipv6 mld-proxy groups`

Mode
- Privileged EXEC
- User EXEC

Field	*Description*
Interface	The interface number of the MLD-Proxy.
Group Address	The IP address of the multicast group.
Last Reporter	The IP address of the host that last sent a membership report for the current group, on the network attached to the MLD-Proxy interface (upstream interface).
Up Time (in secs)	The time elapsed in seconds since last created.
Member State	Possible values are: • **Idle_Member**. The interface has responded to the latest group membership query for this group. • **Delay_Member**. The 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.

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

```
(Routing) #show ipv6 mld-proxy groups

Interface Index.............................. 1/0/3

Group Address    Last Reporter    Up Time   Member State                Filter Mode  Sources
-------------    -------------- ---------- ---------------- ------------- -------
FF1E::1           FE80::100:2.3    00:01:40  DELAY_MEMBER            Exclude         2

FF1E::2           FE80::100:2.3    00:02:40  DELAY_MEMBER            Include         1

FF1E::3           FE80::100:2.3    00:01:40  DELAY_MEMBER            Exclude         0

FF1E::4           FE80::100:2.3    00:02:44  DELAY_MEMBER         Include            4
```

show ipv6 mld-proxy groups detail

Use this command to display information about multicast groups that MLD-Proxy reported.

Format `show ipv6 mld-proxy groups detail`

Mode
- Privileged EXEC
- User EXEC

Field	*Description*
Interface	The interface number of the MLD-Proxy.
Group Address	The IP address of the multicast group.
Last Reporter	The IP address of the host that last sent a membership report for the current group, on the network attached to the MLD-Proxy interface (upstream interface).
Up Time (in secs)	The time elapsed in seconds since last created.
Member State	Possible values are: • **Idle_Member**. The interface has responded to the latest group membership query for this group. • **Delay_Member**. The 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	The time left for a source to get deleted.

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

```
(Routing) #show ipv6 igmp-proxy groups

Interface Index.............................. 1/0/3

Group Address    Last Reporter    Up Time   Member State                Filter Mode  Sources
-------------   ---------------- ----------- ----------------- ------------- -------
FF1E::1           FE80::100:2.3         244        DELAY_MEMBER      Exclude         2

Group Source List             Expiry Time
------------------            ---------------
2001::1                          00:02:40
2001::2                          --------


FF1E::2           FE80::100:2.3        243      DELAY_MEMBER   Include         1

Group Source List             Expiry Time
------------------            ---------------
3001::1                          00:03:32
3002::2                          00:03:32
```

```
FF1E::3           FE80::100:2.3        328      DELAY_MEMBER   Exclude        0

FF1E::4       FE80::100:2.3        255       DELAY_MEMBER   Include         4

Group Source List             Expiry Time
------------------            ---------------
4001::1                                 00:03:40
5002::2                                 00:03:40
4001::2                                 00:03:40
5002::2                                 00:03:40
```

Appendix A: DWS-4000 Log Messages

This chapter lists common log messages that are provided by DWS-4000, along with information regarding the cause of each message. There is no specific action that can be taken per message. When there is a problem being diagnosed, a set of these messages in the event log, along with an understanding of the system configuration and details of the problem) will assist Broadcom in determining the root cause of such a problem.

Note: This chapter is not a complete list of all syslog messages.

The Log Messages chapter includes the following sections:

Core

Table 16: BSP Log Messages

Component	*Message*	*Cause*
BSP	Event(0xaaaaaaaa)	Switch has restarted.
BSP	Starting code...	BSP initialization complete, starting DWS-4000 application.

Table 17: NIM Log Messages

Component	*Message*	*Cause*
NIM	NIM: L7_ATTACH out of order for interface unit x slot x port x	Interface creation out of order.
NIM	NIM: Failed to find interface at unit x slot x port x for event(x)	There is no mapping between the USP and Interface number.
NIM	NIM: L7_DETACH out of order for interface unit x slot x port x	Interface creation out of order.

Table 17: NIM Log Messages (Cont.)

Component	*Message*	*Cause*
NIM	NIM: L7_DELETE out of order for interface unit x slot x port x	Interface creation out of order.
NIM	NIM: event(x),intf(x),component(x), in wrong phase	An event was issued to NIM during the wrong configuration phase (probably Phase 1, 2, or WMU).
NIM	NIM: Failed to notify users of interface change	Event was not propagated to the system.
NIM	NIM: failed to send message to NIM message Queue.	NIM message queue full or non-existent.
NIM	NIM: Failed to notify the components of L7_CREATE event	Interface not created.
NIM	NIM: Attempted event (x), on USP x.x.x before phase 3	A component issued an interface event during the wrong initialization phase.
NIM	NIM: incorrect phase for operation	An API call was made during the wrong initialization phase.
NIM	NIM: Component(x) failed on event(x) for interface	A component responded with a fail indication for an interface event.
NIM	NIM: Timeout event(x), interface remainingMask = xxxx	A component did not respond before the NIM timeout occurred.

Table 18: SIM Log Message

Component	*Message*	*Cause*
SIM	IP address conflict on service port/network port for IP address x.x.x.x. Conflicting host MAC address is xx:xx:xx:xx:xx:xx	This message appears when an address conflict is detected in the LAN for the service port/network port IP.

Table 19: System Log Messages

Component	*Message*	*Cause*
SYSTEM	Configuration file fastpath.cfg size is 0 (zero) bytes	The configuration file could not be read. This message may occur on a system for which no configuration has ever been saved or for which configuration has been erased.
SYSTEM	could not separate SYSAPI_CONFIG_FILENAME	The configuration file could not be read. This message may occur on a system for which no configuration has ever been saved or for which configuration has been erased.
SYSTEM	Building defaults for file *file name* version *version num*	Configuration did not exist or could not be read for the specified feature or file. Default configuration values will be used. The file name and version are indicated.

Table 19: System Log Messages (Cont.)

Component	Message	Cause
SYSTEM	File *filename*: same version (*version num*) but the sizes (*version size – expected version size*) differ	The configuration file which was loaded was of a different size than expected for the version number. This message indicates the configuration file needed to be migrated to the version number appropriate for the code image. This message may appear after upgrading the code image to a more current release.
SYSTEM	Migrating config file *filename* from version *version num* to *version num*	The configuration file identified was migrated from a previous version number. Both the old and new version number are specified. This message may appear after upgrading the code image to a more current release.
SYSTEM	Building Defaults	Configuration did not exist or could not be read for the specified feature. Default configuration values will be used.
SYSTEM	sysapiCfgFileGet failed size = *expected size of file* version = *expected version*	Configuration did not exist or could not be read for the specified feature. This message is usually followed by a message indicating that default configuration values will be used.

Utilities

Table 20: Trap Mgr Log Message

Component	Message	Cause
Trap Mgr	Link Up/Down: unit/slot/port	An interface changed link state.

Table 21: DHCP Filtering Log Messages

Component	Message	Cause
DHCP Filtering	Unable to create r/w lock for DHCP Filtering	Unable to create semaphore used for dhcp filtering configuration structure.
DHCP Filtering	Failed to register with nv Store.	Unable to register save and restore functions for configuration save.
DHCP Filtering	Failed to register with NIM	Unable to register with NIM for interface callback functions.
DHCP Filtering	Error on call to sysapiCfgFileWrite file	Error on trying to save configuration.

Table 22: NVStore Log Messages

Component	*Message*	*Cause*
NVStore	Building defaults for file XXX	A component's configuration file does not exist or the file's checksum is incorrect so the component's default configuration file is built.
NVStore	Error on call to osapiFsWrite routine on file XXX	Either the file cannot be opened or the OS's file I/O returned an error trying to write to the file.
NVStore	File XXX corrupted from file system. Checksum mismatch.	The calculated checksum of a component's configuration file in the file system did not match the checksum of the file in memory.
NVStore	Migrating config file XXX from version Y to Z	A configuration file version mismatch was detected so a configuration file migration has started.

Table 23: RADIUS Log Messages

Component	*Message*	*Cause*
RADIUS	RADIUS: Invalid data length - xxx	The RADIUS Client received an invalid message from the server.
RADIUS	RADIUS: Failed to send the request	A problem communicating with the RADIUS server.
RADIUS	RADIUS: Failed to send all of the request	A problem communicating with the RADIUS server during transmit.
RADIUS	RADIUS: Could not get the Task Sync semaphore!	Resource issue with RADIUS Client service.
RADIUS	RADIUS: Buffer is too small for response processing	RADIUS Client attempted to build a response larger than resources allow.
RADIUS	RADIUS: Could not allocate accounting requestInfo	Resource issue with RADIUS Client service.
RADIUS	RADIUS: Could not allocate requestInfo	Resource issue with RADIUS Client service.
RADIUS	RADIUS: osapiSocketRecvFrom returned error	Error while attempting to read data from the RADIUS server.
RADIUS	RADIUS: Accounting-Response failed to validate, id = xxx	The RADIUS Client received an invalid message from the server.
RADIUS	RADIUS: User (xxx) needs to respond for challenge	An unexpected challenge was received for a configured user.
RADIUS	RADIUS: Could not allocate a buffer for the packet	Resource issue with RADIUS Client service.
RADIUS	RADIUS: Access-Challenge failed to validate, id = xxx	The RADIUS Client received an invalid message from the server.
RADIUS	RADIUS: Failed to validate Message-Authenticator, id = xxx	The RADIUS Client received an invalid message from the server.

Table 23: RADIUS Log Messages (Cont.)

Component	Message	Cause
RADIUS	RADIUS: Access-Accept failed to validate, id = xxx	The RADIUS Client received an invalid message from the server.
RADIUS	RADIUS: Invalid packet length – xxx	The RADIUS Client received an invalid message from the server.
RADIUS	RADIUS: Response is missing Message-Authenticator, id = xxx	The RADIUS Client received an invalid message from the server.
RADIUS	RADIUS: Server address doesn't match configured server	RADIUS Client received a server response from an unconfigured server.

Table 24: TACACS+ Log Messages

Component	Message	Cause
TACACS+	TACACS+: authentication error, no server to contact	TACACS+ request needed, but no servers are configured.
TACACS+	TACACS+: connection failed to server x.x.x.x	TACACS+ request sent to server x.x.x.x but no response was received.
TACACS+	TACACS+: no key configured to encrypt packet for server x.x.x.x	No key configured for the specified server.
TACACS+	TACACS+: received invalid packet type from server.	Received packet type that is not supported.
TACACS+	TACACS+: invalid major version in received packet.	Major version mismatch.
TACACS+	TACACS+: invalid minor version in received packet.	Minor version mismatch.

Table 25: LLDP Log Message

Component	Message	Cause
LLDP	lldpTask(): invalid message type:xx. xxxxxx:xx	Unsupported LLDP packet received.

Table 26: SNTP Log Message

Component	Message	Cause
SNTP	SNTP: system clock synchronized on %s UTC	Indicates that SNTP has successfully synchronized the time of the box with the server.

Table 27: DHCPv6 Client Log Messages

Component	*Message*	*Cause*
DHCP6 Client	ip6Map dhcp add failed.	This message appears when the update of a DHCP leased IP address to IP6Map fails.
DHCP6 Client	osapiNetAddrV6Add failed on interface xxx.	This message appears when the update of a DHCP leased IP address to the kernel IP Stack fails.
DHCP6 Client	Failed to add DNS Server xxx to DNS Client.	This message appears when the update of a DNS6 Server address given by the DHCPv6 Server to the DNS6 Client fails.
DHCP6 Client	Failed to add Domain name xxx to DNS Client.	This message appears when the update of a DNS6 Domain name info given by the DHCPv6 Server to the DNS6 Client fails.

Table 28: DHCPv4 Client Log Messages

Component	*Message*	*Cause*
DHCP4 Client	Unsupported subOption (xxx) in Vendor Specific Option in received DHCP pkt	This message appears when a message is received from the DHCP Server that contains an un-supported Vendor Option.
DHCP4 Client	Failed to acquire an IP address on xxx; DHCP Server did not respond.	This message appears when the DHCP Client fails to lease an IP address from the DHCP Server.
DHCP4 Client	DNS name server entry add failed.	This message appears when the update of a DNS Domain name server info given by the DHCP Server to the DNS Client fails.
DHCP4 Client	DNS domain name list entry addition failed.	This message appears when the update of a DNS Domain name list info given by the DHCP Server to the DNS Client fails.
DHCP4 Client	Interface xxx Link State is Down. Connect the port and try again.	This message appears when the Network protocol is configured with DHCP without any active links in the Management VLAN.

Management

Table 29: SNMP Log Message

Component	Message	Cause
SNMP	EDB Callback: Unit Join: x.	A new unit has joined the stack.

Table 30: EmWeb Log Messages

Component	Message	Cause
EmWeb	EMWEB (Telnet): Max number of Telnet login sessions exceeded	A user attempted to connect via telnet when the maximum number of telnet sessions were already active.
EmWeb	EMWEB (SSH): Max number of SSH login sessions exceeded	A user attempted to connect via SSH when the maximum number of SSH sessions were already active.
EmWeb	Handle table overflow	All the available EmWeb connection handles are being used and the connection could not be made.
EmWeb	*ConnectionType* EmWeb socket accept() failed: errno	Socket accept failure for the specified connection type.
EmWeb	ewsNetHTTPReceive failure in NetReceiveLoop() - closing connection.	Socket receive failure.
EmWeb	EmWeb: connection allocation failed	Memory allocation failure for the new connection.
EmWeb	EMWEB TransmitPending: EWOULDBLOCK error sending data	Socket error on send.
EmWeb	ewaNetHTTPEnd: internal error - handle not in Handle table	EmWeb handle index not valid.
EmWeb	ewsNetHTTPReceive:recvBufCnt exceeds MAX_QUEUED_RECV_BUFS!	The receive buffer limit has been reached. Bad request or DoS attack.
EmWeb	EmWeb accept: XXXX	Accept function for new SSH connection failed. XXXX indicates the error info.

Table 31: CLI_UTIL Log Messages

Component	Message	Cause
CLI_UTIL	Telnet Send Failed errno = 0x%x	Failed to send text string to the telnet client.
CLI_UTIL	osapiFsDir failed	Failed to obtain the directory information from a volume's directory.

Table 32: WEB Log Messages

Component	Message	Cause
WEB	Max clients exceeded	This message is shown when the maximum allowed java client connections to the switch is exceeded.
WEB	Error on send to sockfd XXXX, closing connection	Failed to send data to the java clients through the socket.
WEB	# (XXXX) Form Submission Failed. No Action Taken.	The form submission failed and no action is taken. XXXX indicates the file under consideration.
WEB	ewaFormServe_file_download() - WEB Unknown return code from tftp download result	Unknown error returned while downloading file using TFTP from web interface.
WEB	ewaFormServe_file_upload() - Unknown return code from tftp upload result	Unknown error returned while uploading file using TFTP from web interface.
WEB	Web UI Screen with unspecified access attempted to be brought up	Failed to get application-specific authorization handle provided to EmWeb/ Server by the application in ewsAuthRegister(). The specified web page will be served in read-only mode.

Table 33: CLI_WEB_MGR Log Messages

Component	Message	Cause
CLI_WEB_MGR	File size is greater than 2K	The banner file size is greater than 2K bytes.
CLI_WEB_MGR	No. of rows greater than allowed maximum of XXXX	When the number of rows exceeds the maximum allowed rows.

Table 34: SSHD Log Messages

Component	Message	Cause
SSHD	SSHD: Unable to create the global (data) semaphore	Failed to create semaphore for global data protection.
SSHD	SSHD: Msg Queue is full, event = XXXX	Failed to send the message to the SSHD message queue as message queue is full. XXXX indicates the event to be sent.
SSHD	SSHD: Unknown UI event in message, event = XXXX	Failed to dispatch the UI event to the appropriate SSHD function as it's an invalid event. XXXX indicates the event to be dispatched.
SSHD	sshdApiCnfgrCommand: Failed calling sshdIssueCmd.	Failed to send the message to the SSHD message queue.

Table 35: SSLT Log Messages

Component	*Message*	*Cause*
SSLT	SSLT: Exceeded maximum, ssltConnectionTask	Exceeded maximum allowed SSLT connections.
SSLT	SSLT: Error creating Secure server socket6	Failed to create secure server socket for IPV6.
SSLT	SSLT: Can't connect to unsecure server at XXXX, result = YYYY, errno = ZZZZ	Failed to open connection to unsecure server. XXXX is the unsecure server socket address. YYYY is the result returned from connect function and ZZZZ is the error code.
SSLT	SSLT: Msg Queue is full, event = XXXX	Failed to send the received message to the SSLT message queue as message queue is full. XXXX indicates the event to be sent.
SSLT	SSLT: Unknown UI event in message, event = XXXX	Failed to dispatch the received UI event to the appropriate SSLT function as it's an invalid event. XXXX indicates the event to be dispatched.
SSLT	ssltApiCnfgrCommand: Failed calling ssltIssueCmd.	Failed to send the message to the SSLT message queue.
SSLT	SSLT: Error loading certificate from file XXXX	Failed while loading the SSLcertificate from specified file. XXXX indicates the file from where the certificate is being read.
SSLT	SSLT: Error loading private key from file	Failed while loading private key for SSL connection.
SSLT	SSLT: Error setting cipher list (no valid ciphers)	Failed while setting cipher list.
SSLT	SSLT: Could not delete the SSL semaphores	Failed to delete SSL semaphores during cleanup.of all resources associated with the OpenSSL Locking semaphores.

Table 36: User_Manager Log Messages

Component	*Message*	*Cause*
User_Manager	User Login Failed for XXXX	Failed to authenticate user login. XXXX indicates the username to be authenticated.
User_Manager	Access level for user XXXX could not be determined. Setting to READ_ONLY.	Invalid access level specified for the user. The access level is set to READ_ONLY. XXXX indicates the username.
User_Manager	Could not migrate config file XXXX from version YYYY to ZZZZ. Using defaults.	Failed to migrate the config file. XXXX is the config file name. YYYY is the old version number and ZZZZ is the new version number.

Switching

Table 37: Protected Ports Log Messages

Component	Message	Cause
Protected Ports	Protected Port: failed to save configuration	This appears when the protected port configuration cannot be saved.
Protected Ports	protectedPortCnfgrInitPhase1Process: Unable to create r/w lock for protected Port	This appears when protectedPortCfgRWLock Fails.
Protected Ports	protectedPortCnfgrInitPhase2Process: Unable to register for VLAN change callback	This appears when nimRegisterIntfChange with VLAN fails.
Protected Ports	Cannot add interface xxx to group yyy	This appears when an interface could not be added to a particular group.
Protected Ports	unable to set protected port group	This appears when a dtl call fails to add interface mask at the driver level.
Protected Ports	Cannot delete interface xxx from group yyy	This appears when a dtl call to delete an interface from a group fails.
Protected Ports	Cannot update group YYY after deleting interface XXX	This message appears when an update group for a interface deletion fails.
Protected Ports	Received an interface change callback while not ready to receive it	This appears when an interface change call back has come before the protected port component is ready.

Table 38: IP Subnet VLANS Log Messages

Component	Message	Cause
IP subnet VLANs	ERROR vlanIpSubnetSubnetValid:Invalid subnet	This occurs when an invalid pair of subnet and netmask has come from the CLI.
IP subnet VLANs	IP Subnet Vlans: failed to save configuration	This message appears when save configuration of subnet vlans failed.
IP subnet VLANs	vlanIpSubnetCnfgrInitPhase1Process: Unable to create r/w lock for vlanIpSubnet	This appears when a read/write lock creations fails.
IP subnet VLANs	vlanIpSubnetCnfgrInitPhase2Process: Unable to register for VLAN change callback	This appears when this component unable to register for vlan change notifications.
IP subnet VLANs	vlanIpSubnetCnfgrFiniPhase1Process: could not delete avl semaphore	This appears when a semaphore deletion of this component fails.
IP subnet VLANs	vlanIpSubnetDtlVlanCreate: Failed	This appears when a dtl call fails to add an entry into the table.
IP subnet VLANs	vlanIpSubnetSubnetDeleteApply: Failed	This appears when a dtl fails to delete an entry from the table.
IP subnet VLANs	vlanIpSubnetVlanChangeCallback: Failed to add an Entry	This appears when a dtl fails to add an entry for a vlan add notify event.
IP subnet VLANs	vlanIpSubnetVlanChangeCallback: Failed to delete an Entry	This appears when a dtl fails to delete an entry for an vlan delete notify event.

Table 39: Mac-based VLANs Log Messages

Component	*Message*	*Cause*
MAC based VLANs	MAC VLANs: Failed to save configuration	This message appears when save configuration of Mac vlans failed.
MAC based VLANs	vlanMacCnfgrInitPhase1Process: Unable to create r/w lock for vlanMac	This appears when a read/write lock creations fails.
MAC based VLANs	Unable to register for VLAN change callback	This appears when this component unable to register for vlan change notifications.
MAC based VLANs	vlanMacCnfgrFiniPhase1Process: could not delete avl semaphore	This appears when a semaphore deletion of this component fails.
MAC based VLANs	vlanMacAddApply: Failed to add an entry	This appears when a dtl call fails to add an entry into the table.
MAC based VLANs	vlanMacDeleteApply: Unable to delete an Entry	This appears when a dtl fails to delete an entry from the table.
MAC based VLANs	vlanMacVlanChangeCallback: Failed to add an entry	This appears when a dtl fails to add an entry for a vlan add notify event.
MAC based VLANs	vlanMacVlanChangeCallback: Failed to delete an entry	This appears when a dtl fails to delete an entry for an vlan delete notify event.

Table 40: 802.1X Log Messages

Component	*Message*	*Cause*
802.1X	*function*: Failed calling dot1xIssueCmd	802.1X message queue is full.
802.1X	*function:* EAP message not received from server	RADIUS server did not send required EAP message.
802.1X	*function*: Out of System buffers	802.1X cannot process/transmit message due to lack of internal buffers.
802.1X	*function*: could not set state to *authorized/ unauthorized*, intf xxx	DTL call failed setting authorization state of the port.
802.1X	dot1xApplyConfigData: Unable to *enable/ disable* dot1x in driver	DTL call failed enabling/disabling 802.1X.
802.1X	dot1xSendRespToServer: dot1xRadiusAccessRequestSend failed	Failed sending message to RADIUS server.
802.1X	dot1xRadiusAcceptProcess: error calling radiusAccountingStart, ifIndex = xxx	Failed sending accounting start to RADIUS server.
802.1X	*function*: failed sending terminate cause, intf xxx	Failed sending accounting stop to RADIUS server.

Table 41: IGMP Snooping Log Messages

Component	*Message*	*Cause*
IGMP Snooping	*function*: osapiMessageSend failed	IGMP Snooping message queue is full.
IGMP Snooping	Failed to set global igmp snooping mode to xxx	Failed to set global IGMP Snooping mode due to message queue being full.
IGMP Snooping	Failed to set igmp snooping mode xxx for interface yyy	Failed to set interface IGMP Snooping mode due to message queue being full.
IGMP Snooping	Failed to set igmp mrouter mode xxx for interface yyy	Failed to set interface multicast router mode due to IGMP Snooping message queue being full.
IGMP Snooping	Failed to set igmp snooping mode xxx for vlan yyy	Failed to set VLAN IGM Snooping mode due to message queue being full.
IGMP Snooping	Failed to set igmp mrouter mode%d for interface xxx on Vlan yyy	Failed to set VLAN multicast router mode due to IGMP Snooping message queue being full.
IGMP Snooping	snoopCnfgrInitPhase1Process: Error allocating small buffers	Could not allocate buffers for small IGMP packets.
IGMP Snooping	snoopCnfgrInitPhase1Process: Error allocating large buffers	Could not allocate buffers for large IGMP packets.

Table 42: GARP/GVRP/GMRP Log Messages

Component	*Message*	*Cause*
GARP/GVRP/ GMRP	garpSpanState, garpIfStateChange, GarpIssueCmd, garpDot1sChangeCallBack, garpApiCnfgrCommand, garpLeaveAllTimerCallback, garpTimerCallback: QUEUE SEND FAILURE:	The garpQueue is full, logs specifics of the message content like internal interface number, type of message, etc.
GARP/GVRP/ GMRP	GarpSendPDU: QUEUE SEND FAILURE	The garpPduQueue is full, logs specific of the GPDU, internal interface number, vlan id, buffer handle, etc.
GARP/GVRP/ GMRP	garpMapIntfIsConfigurable, gmrpMapIntfIsConfigurable: Error accessing GARP/GMRP config data for interface %d in garpMapIntfIsConfigurable.	A default configuration does not exist for this interface. Typically a case when a new interface is created and has no pre-configuration.
GARP/GVRP/ GMRP	garpTraceMsgQueueUsage: garpQueue usage has exceeded fifty/eighty/ninety percent	Traces the build up of message queue. Helpful in determining the load on GARP.
GARP/GVRP/ GMRP	gid_destroy_port: Error Removing port %d registration for vlan-mac %d - %02X:%02X:%02X:%02X:%02X:%02X	Mismatch between the gmd (gmrp database) and MFDB.
GARP/GVRP/ GMRP	gmd_create_entry**:** GMRP failure adding MFDB entry: vlan %d and address %s	MFDB table is full.

Table 43: 802.3ad Log Messages

Component	Message	Cause
802.3ad	dot3adReceiveMachine: received default event %x	Received a LAG PDU and the RX state machine is ignoring this LAGPDU.
802.3ad	dot3adNimEventCompletionCallback, dot3adNimEventCreateCompletionCallback: DOT3AD: notification failed for event(%d), intf(%d), reason(%d)	The event sent to NIM was not completed successfully.

Table 44: FDB Log Message

Component	Message	Cause
FDB	fdbSetAddressAgingTimeOut: Failure setting fid %d address aging timeout to %d	Unable to set the age time in the hardware.

Table 45: Double VLAN Tag Log Message

Component	Message	Cause
Double Vlan Tag	dvlantagIntfIsConfigurable: Error accessing dvlantag config data for interface %d	A default configuration does not exist for this interface. Typically a case when a new interface is created and has no pre-configuration.

Table 46: IPv6 Provisioning Log Message

Component	Message	Cause
IPV6 Provisioning	ipv6ProvIntfIsConfigurable: Error accessing IPv6 Provisioning config data for interface %d	A default configuration does not exist for this interface. Typically a case when a new interface is created and has no pre-configuration.

Table 47: MFDB Log Message

Component	Message	Cause
MFDB	mfdbTreeEntryUpdate: entry does not exist	Trying to update a non existing entry.

Table 48: 802.1Q Log Messages

Component	*Message*	*Cause*
802.1Q	dot1qIssueCmd: Unable to send message %d to dot1qMsgQueue for vlan %d - %d msgs in queue	dot1qMsgQueue is full.
802.1Q	dot1qVlanCreateProcess: Attempt to create a vlan with an invalid vlan id %d ; VLAN %d not in range,	This accommodates for reserved vlan ids. i.e. 4094 - x.
802.1Q	dot1qMapIntfIsConfigurable: Error accessing DOT1Q config data for interface %d in dot1qMapIntfIsConfigurable.	A default configuration does not exist for this interface. Typically a case when a new interface is created and has no pre-configuration.
802.1Q	dot1qVlanDeleteProcess: Deleting the default VLAN	Typically encountered during clear Vlan and clear config.
802.1Q	dot1qVlanMemberSetModify, dot1qVlanTaggedMemberSetModify: Dynamic entry %d can only be modified after it is converted to static	If this vlan is a learnt via GVRP then we cannot modify its member set via management.
802.1Q	dtl failure when adding ports to vlan id %d - portMask = %s	Failed to add the ports to VLAN entry in hardware.
802.1Q	dtl failure when deleting ports from vlan id %d - portMask = %s	Failed to delete the ports for a VLAN entry from the hardware.
802.1Q	dtl failure when adding ports to tagged list for vlan id %d - portMask = %s	Failed to add the port to the tagged list in hardware.
802.1Q	dtl failure when deleting ports from tagged list for vlan id %d - portMask = %s"	Failed to delete the port to the tagged list from the hardware.
802.1Q	dot1qTask: unsuccessful return code on receive from dot1qMsgQueue: %08x"	Failed to receive the dot1q message from dot1q message queue.
802.1Q	Unable to apply VLAN creation request for VLAN ID %d, Database reached MAX VLAN count!	Failed to create VLAN ID, VLAN Database reached maximum values.
802.1Q	Attempt to create a vlan (%d) that already exists	Creation of the existing Dynamic VLAN ID from the CLI.
802.1Q	DTL call to create VLAN %d failed with rc %d"	Failed to create VLAN ID in hardware.
802.1Q	Problem unrolling data for VLAN %d	Failed to delete VLAN from the VLAN database after failure of VLAN hardware creation.
802.1Q	VLan %d does not exist	Failed to delete VLAN entry.
802.1Q	VLan %d requestor type %d does not exist	Failed to delete dynamic VLAN ID if the given requestor is not valid.
802.1Q	Can not delete the VLAN, Some unknown component has taken the ownership!	Failed to delete, as some unknown component has taken the ownership.
802.1Q	Not valid permission to delete the VLAN %d requestor %d	Failed to delete the VLAN ID as the given requestor and VLAN entry status are not same.
802.1Q	VLAN Delete Call failed in driver for vlan %d	Failed to delete VLAN ID from the hardware.

Table 48: 802.1Q Log Messages (Cont.)

Component	*Message*	*Cause*
802.1Q	Problem deleting data for VLAN %d	Failed to delete VLAN ID from the VLAN database.
802.1Q	Dynamic entry %d can only be modified after it is converted to static	Failed to modify the VLAN group filter
802.1Q	Cannot find vlan %d to convert it to static	Failed to convert Dynamic VLAN to static VLAN. VLAN ID not exists.
802.1Q	Only Dynamically created vlans can be converted	Error while trying to convert the static created VLAN ID to static.
802.1Q	Cannot modify tagging of interface %s to non existence vlan %d"	Error for a given interface sets the tagging property for all the vlans in the vlan mask.
802.1Q	Error in updating data for VLAN %d in VLAN database	Failed to add VLAN entry into VLAN database.
802.1Q	DTL call to create VLAN %d failed with rc %d	Failed to add VLAN entry in hardware.
802.1Q	Not valid permission to delete the VLAN %d	Failed to delete static VLAN ID. Invalid requestor.
802.1Q	Attempt to set access vlan with an invalid vlan id %d	Invalid VLAN ID.
802.1Q	Attempt to set access vlan with (%d) that does not exist	VLAN ID not exists.
802.1Q	VLAN create currently underway for VLAN ID %d	Creating a VLAN which is already under process of creation.
802.1Q	VLAN ID %d is already exists as static VLAN	Trying to create already existing static VLAN ID.
802.1Q	Cannot put a message on dot1q msg Queue, Returns:%d	Failed to send Dot1q message on Dot1q message Queue.
802.1Q	Invalid dot1q Interface: %s	Failed to add VLAN to a member of port.
802.1Q	Cannot set membership for user interface %s on management vlan %d	Failed to add VLAN to a member of port.
802.1Q	Incorrect tagmode for vlan tagging. tagmode: %d Interface: %s	Incorrect tagmode for VLAN tagging.
802.1Q	Cannot set tagging for interface %d on non existent vlan %d"	The VLAN ID does not exist.
802.1Q	Cannot set tagging for interface %d which is not a member of vlan %d	Failure in Setting the tagging configuration for a interface on a range of vlan.
802.1Q	VLAN create currently underway for VLAN ID %d"	Trying to create the VLAN ID which is already under process of creation.
802.1Q	VLAN ID %d already exists	Trying to create the VLAN ID which is already exists.
802.1Q	Failed to delete, Default VLAN %d cannot be deleted	Trying to delete Default VLAN ID.
802.1Q	Failed to delete, VLAN ID %d is not a static VLAN	Trying to delete Dynamic VLAN ID from CLI.
802.1Q	Requestor %d attempted to release internal vlan %d: owned by %d	-

Table 49: 802.1S Log Messages

Component	Message	Cause
802.1S	dot1sIssueCmd: Dot1s Msg Queue is full!!!!Event: %u, on interface: %u, for instance: %u	The message Queue is full.
802.1S	dot1sStateMachineRxBpdu(): Rcvd BPDU Discarded	The current conditions, like port is not enabled or we are currently not finished processing another BPDU on the same interface, does not allow us to process this BPDU.
802.1S	dot1sBpduTransmit(): could not get a buffer	Out of system buffers.

Table 50: Port Mac Locking Log Message

Component	Message	Cause
Port Mac Locking	pmlMapIntfIsConfigurable: Error accessing PML config data for interface %d in pmlMapIntfIsConfigurable.	A default configuration does not exist for this interface. Typically a case when a new interface is created and has no pre-configuration.

Table 51: Protocol-based VLANs Log Messages

Component	Message	Cause
Protocol Based VLANs	pbVlanCnfgrInitPhase2Process: Unable to register NIM callback	Appears when nimRegisterIntfChange fails to register pbVlan for link state changes.
Protocol Based VLANs	pbVlanCnfgrInitPhase2Process: Unable to register pbVlan callback with vlans	Appears when vlanRegisterForChange fails to register pbVlan for vlan changes.
Protocol Based VLANs	pbVlanCnfgrInitPhase2Process: Unable to register pbVlan callback with nvStore	Appears when nvStoreRegister fails to register save and restore functions for configuration save.

QoS

Table 52: ACL Log Messages

Component	*Message*	*Cause*
ACL	Total number of ACL rules (x) exceeds max (y) on intf i.	The combination of all ACLs applied to an interface has resulted in requiring more rules than the platform supports.
ACL	ACL *name*, rule *x*: This rule is not being logged	The ACL configuration has resulted in a requirement for more logging rules than the platform supports. The specified rule is functioning normally except for the logging action.
ACL	aclLogTask: error logging ACL rule trap for correlator *number*	The system was unable to send an SNMP trap for this ACL rule which contains a logging attribute.
ACL	IP ACL *number*: Forced truncation of one or more rules during config migration	While processing the saved configuration, the system encountered an ACL with more rules than is supported by the current version. This may happen when code is updated to a version supporting fewer rules per ACL than the previous version.

Table 53: CoS Log Message

Component	*Message*	*Cause*
COS	cosCnfgrInitPhase3Process: Unable to apply saved config -- using factory defaults	The COS component was unable to apply the saved configuration and has initialized to the factory default settings.

Table 54: DiffServ Log Messages

Component	*Message*	*Cause*
DiffServ	diffserv.c 165: diffServRestore Failed to reset DiffServ. Recommend resetting device	While attempting to clear the running configuration an error was encountered in removing the current settings. This may lead to an inconsistent state in the system and resetting is advised.
DiffServ	Policy invalid for service intf: "policy *name*, interface *x*, direction *y*	The DiffServ policy definition is not compatible with the capabilities of the interface specified. Check the platform release notes for information on configuration limitations.

Routing/IPv6 Routing

Table 55: DHCP Relay Log Messages

Component	*Message*	*Cause*
DHCP relay	REQUEST hops field more than config value	The DHCP relay agent has processed a DHCP request whose HOPS field is larger than the maximum value allowed. The relay agent will not forward a message with a hop count greater than 4.
DHCP relay	Request's seconds field less than the config value	The DHCP relay agent has processed a DHCP request whose SECS field is larger than the configured minimum wait time allowed.
DHCP relay	processDhcpPacket: invalid DHCP packet type: %u\n	The DHCP relay agent has processed an invalid DHCP packet. Such packets are discarded by the relay agent.

Table 56: OSPFv2 Log Messages

Component	*Message*	*Cause*
OSPFv2	Best route client deregistration failed for OSPF Redist	OSPFv2 registers with the IPv4 routing table manager (RTO) to be notified of best route changes. There are cases where OSPFv2 deregisters more than once, causing the second deregistration to fail. The failure is harmless.
OSPFv2	XX_Call() failure in _checkTimers for thread 0x869bcc0	An OSPFv2 timer has fired but the message queue that holds the event has filled up. This is normally a fatal error.
OSPFv2	Warning: OSPF LSDB is 90% full (22648 LSAs).	OSPFv2 limits the number of Link State Advertisements (LSAs) that can be stored in the link state database (LSDB). When the database becomes 90 or 95 percent full, OSPFv2 logs this warning. The warning includes the current size of the database.
OSPFv2	The number of LSAs, 25165, in the OSPF LSDB has exceeded the LSDB memory allocation.	When the OSPFv2 LSDB becomes full, OSPFv2 logs this message. OSPFv2 reoriginates its router LSAs with the metric of all non-stub links set to the maximum value to encourage other routers to not compute routes through the overloaded router.
OSPFv2	Dropping the DD packet because of MTU mismatch	OSPFv2 ignored a Database Description packet whose MTU is greater than the IP MTU on the interface where the DD was received.
OSPFv2	LSA Checksum error in LsUpdate, dropping LSID 1.2.3.4 checksum 0x1234.	OSPFv2 ignored a received link state advertisement (LSA) whose checksum was incorrect.

Table 57: OSPFv3 Log Messages

Component	*Message*	*Cause*
OSPFv3	Best route client deregistration failed for OSPFv3 Redist	OSPFv3 registers with the IPv6 routing table manager (RTO6) to be notified of best route changes. There are cases where OSPFv3 deregisters more than once, causing the second deregistration to fail. The failure is harmless.
OSPFv3	Warning: OSPF LSDB is 90% full (15292 LSAs).	OSPFv3 limits the number of Link State Advertisements (LSAs) that can be stored in the link state database (LSDB). When the database becomes 90 or 95 percent full, OSPFv3 logs this warning. The warning includes the current size of the database.
OSPFv3	The number of LSAs, 16992, in the OSPF LSDB has exceeded the LSDB memory allocation.	When the OSPFv3 LSDB becomes full, OSPFv3 logs this message. OSPFv3 reoriginates its router LSAs with the R-bit clear indicating that OSPFv3 is overloaded.
OSPFv3	LSA Checksum error detected for LSID 1.2.3.4 checksum 0x34f5. OSPFv3 Database may be corrupted.	OSPFv3 periodically verifies the checksum of each LSA in memory. OSPFv3 logs this.

Table 58: Routing Table Manager Log Messages

Component	*Message*	*Cause*
RTO	RTO is no longer full. Routing table contains xxx best routes, xxx total routes, xxx reserved local routes.	When the number of best routes drops below full capacity, RTO logs this notice. The number of bad adds may give an indication of the number of route adds that failed while RTO was full, but a full routing table is only one reason why this count is incremented.
RTO	RTO is full. Routing table contains xxx best routes, xxx total routes, xxx reserved local routes. The routing table manager stores a limited number of best routes. The count of total routes includes alternate routes, which are not installed in hardware.	The routing table manager, also called RTO, stores a limited number of best routes, based on hardware capacity. When the routing table becomes full, RTO logs this alert. The count of total routes includes alternate routes, which are not installed in hardware.

Table 59: VRRP Log Messages

Component	*Message*	*Cause*
VRRP	VRRP packet of size xxx dropped. Min VRRP packet size is xxx; Max VRRP packet size is xxx.	This message appears when there is flood of VRRP messages in the network.
VRRP	VR xxx on interface xxx started as xxx.	This message appears when the Virtual router is started in the role of a Master or a Backup.
VRRP	This router is the IP address owner for virtual router xxx on interface xxx. Setting the virtual router priority to xxx.	This message appears when the address ownership status for a specific VR is updated. If this router is the address owner for the VR, set the VR's priority to MAX priority (as per RFC 3768). If the router is no longer the address owner, revert the priority.

Table 60: ARP Log Message

Component	*Message*	*Cause*
ARP	IP address conflict on interface xxx for IP address yyy. Conflicting host MAC address is zzz.	When an address conflict is detected for any IP address on the switch upon reception of ARP packet from another host or router.

Table 61: RIP Log Message

Component	*Message*	*Cause*
RIP	RIP : discard response from xxx via unexpected interface	When RIP response is received with a source address not matching the incoming interface’s subnet.

Multicast

Table 62: IGMP/MLD Log Messages

Component	*Message*	*Cause*
IGMP/MLD	MGMD Protocol Heap Memory Init Failed; Family – xxx.	MGMD Heap memory initialization Failed for the specified address family. This message appears when trying to enable MGMD Protocol.
IGMP/MLD	MGMD Protocol Heap Memory De-Init Failed; Family – xxx.	MGMD Heap memory de-initialization Failed for the specified address family. This message appears when trying to disable MGMD (IGMP/MLD) Protocol. As a result of this, the subsequent attempts to enable/ disable MGMD will also fail.
IGMP/MLD	MGMD Protocol Initialization Failed; Family – xxx.	MGMD protocol initialization sequence Failed. This could be due to the non-availability of some resources. This message appears when trying to enable MGMD Protocol.
IGMP/MLD	MGMD All Routers Address - xxx Set to the DTL Mcast List Failed; Mode – xxx, intf – xxx.	This message appears when trying to enable/ disable MGMD Protocol.
IGMP/MLD	MGMD All Routers Address - xxx Add to the DTL Mcast List Failed.	MGMD All Routers Address addition to the local multicast list Failed. As a result of this, MGMD Multicast packets with this address will not be received at the application.
IGMP/MLD	MGMD All Routers Address – xxx Delete from the DTL Mcast List Failed.	MGMD All Routers Address deletion from the local multicast list Failed. As a result of this, MGMD Multicast packets are still received at the application though MGMD is disabled.
IGMP/MLD	MLDv2 GroupAddr-[FF02::16] Enable with Interpeak Stack Failed; rtrIfNum - xxx, intf – xxx.	Registration of this Group address with the Interpeak stack failed. As a result of this, MLDv2 packets will not be received at the application.
IGMP/MLD	MGMD Group Entry Creation Failed; grpAddr - xxx, rtrIfNum – xxx.	The specified Group Address registration on the specified router interface failed.
IGMP/MLD	MGMD Socket Creation/Initialization Failed for addrFamily – xxx.	MGMD Socket Creation/options Set Failed. As a result of this, the MGMD Control packets cannot be sent out on an interface.

Table 63: IGMP-Proxy Log Messages

Component	*Message*	*Cause*
IGMP-Proxy/ MLD-Proxy	MGMD-Proxy Protocol Initialization Failed; Family – xxx.	MGMD-Proxy protocol initialization sequence Failed. This could be due to the non-availability of some resources. This message appears when trying to enable MGMD-Proxy Protocol.
IGMP-Proxy/ MLD-Proxy	MGMD-Proxy Protocol Heap Memory De-Init Failed; Family – xxx.	MGMD-Proxy Heap memory de-initialization is Failed for the specified address family. This message appears when trying to disable MGMD-Proxy Protocol. As a result of this, the subsequent attempts to enable/disable MGMD-Proxy will also fail.
IGMP-Proxy/ MLD-Proxy	MGMD Proxy Route Entry Creation Failed; grpAddr - xxx, srcAddr – xxx, rtrIfNum – xxx.	Registration of the Multicast Forwarding entry for the specified Source and Group Address Failed when MGMD-Proxy is used.

Table 64: PIM-SM Log Messages

Component	*Message*	*Cause*
PIMSM	Non-Zero SPT/Data Threshold Rate – xxx is currently Not Supported on this platform.	This message appears when the user tries to configure the PIMSM SPT threshold value.
PIMSM	PIMSM Protocol Heap Memory Init Failed; Family – xxx.	PIMSM Heap memory initialization Failed for the specified address family. This message appears when trying to enable PIMSM Protocol.
PIMSM	PIMSM Protocol Heap Memory De-Init Failed; Family –xxx.	PIMSM Heap memory de-initialization Failed for the specified address family. This message appears when trying to disable PIMSM Protocol. As a result of this, the subsequent attempts to enable/disable PIMSM will also fail.
PIMSM	PIMSM Protocol Initialization Failed; Family – xxx.	PIMSM protocol initialization sequence Failed. This could be due to the non-availability of some resources. This message appears when trying to enable PIMSM Protocol.
PIMSM	PIMSM Protocol De-Initialization Failed; Family – xxx.	PIMSM protocol de-initialization sequence Failed. This message appears when trying to disable PIMSM Protocol.
PIMSM	PIMSM SSM Range Table is Full.	PIMSM SSM Range Table is Full. This message appears when the protocol cannot accommodate new SSM registrations.
PIMSM	PIM All Routers Address – xxx Delete from the DTL Mcast List Failed for intf – xxx.	PIM All Routers Address deletion from the local multicast list Failed. As a result of this, PIM Multicast packets are still received at the application though PIM is disabled.

Table 64: PIM-SM Log Messages (Cont.)

Component	Message	Cause
PIMSM	PIM All Routers Address - xxx Add to the DTL Mcast List Failed for intf – xxx.	PIM All Routers Address addition to the local multicast list Failed. As a result of this, PIM Multicast packets with this address will not be received at the application.
PIMSM	Mcast Forwarding Mode Disable Failed for intf – xxx.	Multicast Forwarding Mode Disable Failed. As a result of this, Multicast packets are still received at the application though no protocol is enabled.
PIMSM	Mcast Forwarding Mode Enable Failed for intf – xxx.	Multicast Forwarding Mode Enable Failed. As a result of this, Multicast packets will not be received at the application though a protocol is enabled.
PIMSM	PIMSMv6 Socket Memb'ship Enable Failed for rtrIfNum - xxx.	PIMSMv6 Socket Creation/options Set with Kernel IP Stack Failed. As a result of this, the PIM Control packets cannot be received on the interface.
PIMSM	PIMSMv6 Socket Memb'ship Disable Failed for rtrIfNum – xxx.	PIMSMv6 Socket Creation/options Disable with Kernel IP Stack Failed. As a result of this, the PIM Control packets are still received on the interface at the application though no protocol is enabled.
PIMSM	PIMSM (S,G,RPt) Table Max Limit – xxx Reached; Cannot accommodate any further routes.	PIMSM Multicast Route table (S,G,RPt) has reached maximum capacity and cannot accommodate new registrations anymore.
PIMSM	PIMSM (S,G) Table Max Limit - xxx Reached; Cannot accommodate any further routes.	PIMSM Multicast Route table (S,G) has reached maximum capacity and cannot accommodate new registrations anymore.
PIMSM	PIMSM (*,G) Table Max Limit - xxx Reached; Cannot accommodate any further routes.	PIMSM Multicast Route table (*,G) has reached maximum capacity and cannot accommodate new registrations anymore.

Table 65: PIM-DM Log Messages

Component	Message	Cause
PIMDM	PIMDM Protocol Heap Memory Init Failed; Family – xxx.	PIMDM Heap memory initialization Failed for the specified address family. This message appears when trying to enable PIMDM Protocol.
PIMDM	PIMDM Protocol Heap Memory De-Init Failed; Family –xxx.	PIMDM Heap memory de-initialization Failed for the specified address family. This message appears when trying to disable PIMDM Protocol. As a result of this, the subsequent attempts to enable/disable PIMDM will also fail.
PIMDM	PIMDM Protocol Initialization Failed; Family –xxx.	PIMDM protocol initialization sequence Failed. This could be due to the non-availability of some resources. This message appears when trying to enable PIMDM Protocol.

Table 65: PIM-DM Log Messages (Cont.)

Component	*Message*	*Cause*
PIMDM	PIMDM Protocol De-Initialization Failed; Family – xxx.	PIMDM protocol de-initialization sequence Failed. This message appears when trying to disable PIMDM Protocol.
PIMDM	PIM All Routers Address – xxx Delete from the DTL Mcast List Failed for intf – xxx.	PIM All Routers Address deletion from the local multicast list Failed. As a result of this, PIM Multicast packets are still received at the application though PIM is disabled.
PIMDM	PIM All Routers Address - xxx Add to the DTL Mcast List Failed for intf – xxx.	PIM All Routers Address addition to the local multicast list Failed. As a result of this, PIM Multicast packets with this address will not be received at the application.
PIMDM	Mcast Forwarding Mode Disable Failed for intf – xxx.	Multicast Forwarding Mode Disable Failed. As a result of this, Multicast packets are still received at the application though no protocol is enabled.
PIMDM	Mcast Forwarding Mode Enable Failed for intf – xxx.	Multicast Forwarding Mode Enable Failed. As a result of this, Multicast packets will not be received at the application though a protocol is enabled.
PIMDM	PIMDMv6 Socket Memb'ship Enable Failed for rtrIfNum - xxx.	PIMDMv6 Socket Creation/options Set with Kernel IP Stack Failed. As a result of this, the PIM Control packets cannot be received on the interface.
PIMDM	PIMDMv6 Socket Memb'ship Disable Failed for rtrIfNum – xxx.	PIMDMv6 Socket Creation/options Disable with Kernel IP Stack Failed. As a result of this, the PIM Control packets are still received on the interface at the application though no protocol is enabled.
PIMDM	PIMDM FSM Action Invoke Failed; rtrIfNum - xxx Out of Bounds for Event – xxx.	The PIMDM FSM Action invocation Failed due to invalid Routing interface number. In such cases, the FSM Action routine can never be invoked which may result in abnormal behavior. The failed FSM-name can be identified from the specified Event name.
PIMDM	PIMDM Socket Initialization Failed for addrFamily - xxx.	PIMDM Socket Creation/options Set Failed. As a result of this, the PIM Control packets cannot be sent out on an interface.
PIMDM	PIMDMv6 Socket Memb'ship Enable Failed for rtrIfNum - xxx.	Socket options Set to enable the reception of PIMv6 packets Failed. As a result of this, the PIMv6 packets will not be received by the application.
PIMDM	PIMDMv6 Socket Memb'ship Disable Failed for rtrIfNum – xxx.	PIMDMv6 Socket Creation/options Disable with Kernel IP Stack Failed. As a result of this, the PIMv6 Control packets are still received on the interface at the application though no protocol is enabled.
PIMDM	PIMDM MRT Table Max Limit - xxx Reached; Cannot accommodate any further routes.	PIMDM Multicast Route table (S,G) has reached maximum capacity and cannot accommodate new registrations anymore.

Table 66: DVMRP Log Messages

Component	*Message*	*Cause*
DVMRP	DVMRP Heap memory initialization is Failed for the specified address family.	This message appears when trying to enable DVMRP Protocol
DVMRP	DVMRP Heap memory de-initialization is Failed for the specified address family.	This message appears when trying to disable DVMRP Protocol. As a result of this, the subsequent attempts to enable/disable DVMRP will also fail.
DVMRP	DVMRP protocol initialization sequence Failed.	This could be due to the non-availability of some resources. This message appears when trying to enable DVMRP Protocol.
DVMRP	DVMRP All Routers Address - xxx Delete from the DTL Mcast List Failed for intf – xxx.	DMVRP All Routers Address deletion from the local multicast list Failed. As a result of this, DVMRP Multicast packets are still received at the application though DVMRP is disabled.
DVMRP	Mcast Forwarding Mode Disable Failed for intf – xxx.	The Multicast Forwarding mode Disable Failed for this routing interface.
DVMRP	DVMRP All Routers Address - xxx Add to the DTL Mcast List Failed for intf – xxx.	DMVRP All Routers Address addition to the local multicast list Failed. As a result of this, DVMRP Multicast packets with this address will not be received at the application.
DVMRP	Mcast Forwarding Mode Enable Failed for intf – xxx.	The Multicast Forwarding mode Enable Failed for this routing interface. As a result of this, the ability to forward Multicast packets does not function on this interface.
DVMRP	DVMRP Probe Control message Send Failed on rtrIfNum – xxx.	DVMRP Probe control message send failed. This could mostly be because of a Failure return status of the socket call sendto(). As a result of this, the DVMRP neighbor could be lost in the neighboring DVMRP routers.
DVMRP	DVMRP Prune Control message Send Failed; rtrIfNum – xxx.	Neighbor - %s, SrcAddr - %s, GrpAddr - %s DVMRP Prune control message send failed. This could mostly be because of a Failure return status of the socket call sendto(). As a result of this, the unwanted multicast traffic is still received and forwarded.
DVMRP	DVMRP Probe Control message Send Failed on rtrIfNum –xxx.	DVMRP Probe control message send failed. This could mostly be because of a Failure return status of the socket call sendto(). As a result of this, the DVMRP neighbor could be lost in the neighboring DVMRP routers.

Stacking

Table 67: EDB Log Message

Component	*Message*	*Cause*
EDB	EDB Callback: Unit Join: *num*.	Unit *num* has joined the stack.

Technologies

Table 68: Broadcom Error Messages

Component	*Message*	*Cause*
Broadcom	Invalid USP unit = x, slot = x, port = x	A port was not able to be translated correctly during the receive.
Broadcom	In hapiBroadSystemMacAddress call to 'bcm_l2_addr_add' - FAILED : x	Failed to add an L2 address to the MAC table. This should only happen when a hash collision occurs or the table is full.
Broadcom	Failed installing mirror action - rest of the policy applied successfully	A previously configured probe port is not being used in the policy. The release notes state that only a single probe port can be configured.
Broadcom	Policy x does not contain rule x	The rule was not added to the policy due to a discrepancy in the rule count for this specific policy. Additionally, the message can be displayed when an old rule is being modified, but the old rule is not in the policy.
Broadcom	ERROR: policy x, tmpPolicy x, size x, data x x x x x x x x	An issue installing the policy due to a possible duplicate hash.
Broadcom	ACL x not found in internal table	Attempting to delete a non-existent ACL.
Broadcom	ACL internal table overflow	Attempting to add an ACL to a full table.
Broadcom	In hapiBroadQosCosQueueConfig, Failed to configure minimum bandwidth. Available bandwidth x	Attempting to configure the bandwidth beyond it's capabilities.
Broadcom	USL: failed to put sync response on queue	A response to a sync request was not enqueued. This could indicate that a previous sync request was received after it was timed out.
Broadcom	USL: failed to sync ipmc table on unit = x	Either the transport failed or the message was dropped.
Broadcom	usl_task_ipmc_msg_send(): failed to send with x	Either the transport failed or the message was dropped.
Broadcom	USL: No available entries in the STG table	The Spanning Tree Group table is full in USL.

Table 68: Broadcom Error Messages (Cont.)

Component	*Message*	*Cause*
Broadcom	USL: failed to sync stg table on unit = x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued.
Broadcom	USL: A Trunk doesn't exist in USL	Attempting to modify a Trunk that doesn't exist.
Broadcom	USL: A Trunk being created by bcmx already existed in USL	Possible synchronization issue between the application, hardware, and sync layer.
Broadcom	USL: A Trunk being destroyed doesn't exist in USL	Possible synchronization issue between the application, hardware, and sync layer.
Broadcom	USL: A Trunk being set doesn't exist in USL	Possible synchronization issue between the application, hardware, and sync layer.
Broadcom	USL: failed to sync trunk table on unit = x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued.
Broadcom	USL: Mcast entry not found on a join	Possible synchronization issue between the application, hardware, and sync layer.
Broadcom	USL: Mcast entry not found on a leave	Possible synchronization issue between the application, hardware, and sync layer.
Broadcom	USL: failed to sync dvlan data on unit = x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued.
Broadcom	USL: failed to sync policy table on unit = x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued.
Broadcom	USL: failed to sync VLAN table on unit = x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued.
Broadcom	Invalid LAG id x	Possible synchronization issue between the BCM driver and HAPI.
Broadcom	Invalid uport calculated from the BCM uport bcmx_l2_addr->lport = x	Uport not valid from BCM driver.
Broadcom	Invalid USP calculated from the BCM uport\nbcmx_l2_addr->lport = x	USP not able to be calculated from the learn event for BCM driver.
Broadcom	Unable to insert route R/P	Route R with prefix P could not be inserted in the hardware route table. A retry will be issued.
Broadcom	Unable to Insert host H	Host H could not be inserted in hardware host table. A retry will be issued.
Broadcom	USL: failed to sync L3 Intf table on unit = x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued.
Broadcom	USL: failed to sync L3 Host table on unit = x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued.

Table 68: Broadcom Error Messages (Cont.)

Component	Message	Cause
Broadcom	USL: failed to sync L3 Route table on unit = x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued.
Broadcom	USL: failed to sync initiator table on unit = x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued.
Broadcom	USL: failed to sync terminator table on unit = x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued.
Broadcom	USL: failed to sync ip-multicast table on unit = x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued.

O/S Support

Table 69: OSAPI VxWorks Log Messages

Component	Message	Cause
OSAPI VxWorks	ftruncate failed – File resides on a read-only file system.	ftruncate is called to correctly set the file's size in the file system after a write. The file system is R/W so this msg indicates the file system may be corrupted.
OSAPI VxWorks	ftruncate failed – File is open for reading only.	ftruncate is called to correctly set the file's size in the file system after a write. The file is opened for R/W so this msg indicates the file system may be corrupted.
OSAPI VxWorks	ftruncate failed – File descriptor refers to a file on which this operation is impossible.	ftruncate is called to correctly set the file's size in the file system after a write. This msg indicates the file system may be corrupted.
OSAPI VxWorks	ftruncate failed – Returned an unknown code in errno.	ftruncate is called to correctly set the file's size in the file system after a write. This msg indicates the file system may be corrupted.
OSAPI VxWorks	ping: bad host!	The address requested to ping can not be converted to an Internet address.
OSAPI VxWorks	osapiTaskDelete: Failed for (XX) error YYY	The requested task can not be deleted because: the requested deletion is called from an ISR, the task is already deleted, or the task ID is invalid.
OSAPI VxWorks	osapiCleanupIf: NetIPGet	During the call to remove the interface from the route table, the attempt to get an ipv4 interface address from the stack failed.
OSAPI VxWorks	osapiCleanupIf: NetMaskGet	During the call to remove the interface from the route table, the attempt to get the ipv4 interface mask from the stack failed.

Table 69: OSAPI VxWorks Log Messages (Cont.)

Component	Message	Cause
OSAPI VxWorks	osapiCleanupIf: NetIpDel	During the call to remove the interface from the route table, the attempt to delete the primary ipv4 address from the stack failed.
OSAPI VxWorks	osapiSemaTake failed	The requested semaphore can not be taken because: the call is made from an ISR or the semaphore ID is invalid.

Table 70: Linux BSP Log Message

Component	Message	Cause
Linux BSP	rc = 10	Second message logged at bootup, right after *Starting code…. Always* logged.

Table 71: OSAPI Linux Log Messages

Component	Message	Cause
OSAPI Linux	osapiNetLinkNeighDump: could not open socket! - or – ipstkNdpFlush: could not open socket! – or – osapiNetlinkDumpOpen: unable to bind socket! errno = XX	Couldn't open a netlink socket. Make sure "ARP Daemon support" (CONFIG_ARPD) is enabled in the Linux kernel, if the reference kernel binary is not being used.
OSAPI Linux	ipstkNdpFlush: sending delete failed	Failed when telling the kernel to delete a neighbor table entry (the message is incorrect).
OSAPI Linux	unable to open /proc/net/ipv6/conf/default/hop_limit	IPv6 MIB objects read, but /proc filesystem is not mounted, or running kernel does not have IPV6 support.
OSAPI Linux	osapimRouteEntryAdd, errno XX adding 0xYY to ZZ – or – osapimRouteEntryDelete, errno XX deleting 0xYY from ZZ	Error adding or deleting an IPv4 route (listed in hex as YY), on the interface with Linux name ZZ Error code can be looked up in errno.h.
OSAPI Linux	l3intfAddRoute: Failed to Add Route – or – l3intfDeleteRoute: Failed to Delete Route	Error adding or deleting a default gateway in the kernel's routing table (the function is really osapiRawMRouteAdd()/Delete()).
OSAPI Linux	osapiNetIfConfig: ioctl on XX failed: addr: 0xYY, err: ZZ – or – osapiNetIPSet: ioctl on XX failed: addr: 0x%YY	Failed trying to set the IP address (in hex as YY) of the interface with Linux name XX, and the interface does not exist. Sometimes this is a harmless race condition (e.g. we try to set address 0 when DHCPing on the network port (dtl0) at bootup, before it's created using TAP).
OSAPI Linux	ping: sendto error	Trouble sending an ICMP echo request packet for the UI ping command. Maybe there was no route to that network.

Table 71: OSAPI Linux Log Messages (Cont.)

Component	*Message*	*Cause*
OSAPI Linux	Failed to Create Interface	Out of memory at system initialization time.
OSAPI Linux	TAP Unable to open XX	The /dev/tap file is missing, or, if not using the reference kernel binary, the kernel is missing “Universal TUN/TAP device driver support” (CONFIG_TUN).
OSAPI Linux	Tap monitor task is spinning on select failures – then – Tap monitor select failed: XX	Trouble reading the /dev/tap device, check the error message XX for details.
OSAPI Linux	Log_Init: log file error - creating new log file	This pertains to the “event log” persistent file in flash. Either it did not exist, or had a bad checksum.
OSAPI Linux	Log_Init: Flash (event) log full; erasing	Event log file has been cleared; happens at boot time.
OSAPI Linux	Log_Init: Corrupt event log; erasing	Event log file had a non-blank entry after a blank entry; therefore, something was messed up.
OSAPI Linux	Failed to Set Interface IP Address – or – IP Netmask – or – Broadcast Address – or – Flags – or – Hardware Address – or – Failed to Retrieve Interface Flags	Trouble adding VRRP IP or MAC address(es) to a Linux network interface.

Appendix B: List of Commands