2-Port and 6-Port Wireless Access Controller

EWS4502
EWS4606

Software Release v1.3.0.47

CLI Command Reference

www.edge-core.com

CLI Command Reference

EWS4502 Wireless Access Controller
with 2 1000BASE-T (RJ-45) Ports

EWS4606 Wireless Access Controller
with 6 1000BASE-T (RJ-45) Ports

FW1.3.0.47
E092016/ST-R02
150200001195A

Table of Contents

Table of Contents

List of Tables

About This Document

This document describes command-line interface (CLI) commands you use to view and configure EWS4502/EWS4606 software on a wireless controller switch platform. 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.

Audience

This document is for system administrators who configure and operate systems using EWS4502/EWS4606 software. It provides an understanding of the configuration options of the EWS4502/EWS4606 software.

Software engineers who integrate EWS4502/EWS4606 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 EWS4502/EWS4606 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.

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`

Table 1: Typographical Conventions (Cont.)

Symbol	*Description*	*Example*
[{ }] Braces within square brackets	Optional parameter values. Indicates a choice within an optional element.	`[{choice1 | choice2}]`

Revision History

This section summarizes the changes in each revision of this guide.

Revision	*Date*	*Change Description*
DCSS Software v1.3.0.47	9/12/2016	**New:** • "IP-ACL Commands" on page 287 • "WIFI Scheduler Commands" on page 290 • "Rate Limit Commands" on page 294
DCSS Software v1.2.0.5	4/05/2015	**Updated:** • "EWS4502/EWS4606 Modules" on page 20 • "Using CLI Help" on page 26 • "show serial" on page 32 • "user" on page 96 • "interface" on page 76 • "ping ipv6" on page 206 • "agetime" on page 216 • "show wireless switch status" on page 229 • "show wireless ap image availability" on page 237 • "show wireless known-client" on page 238 • "show wireless channel-plan history" on page 246 • "show wireless channel-plan proposed" on page 246 • "show wireless power-plan proposed" on page 247 • "security mode" on page 260 • "vap-tun-switch-type" on page 274 • "show wireless network" on page 284 • "accton-ap reset-mode" on page 298 • "show wireless ap profile radio" on page 323 • "clear wireless ap neighbors" on page 337 • "show wireless ap radio status" on page 340 • "show wireless ap rf-scan status" on page 356 • "show wireless client status" on page 361 • "show wireless ssid client status" on page 367 • "show wireless switch client status" on page 368 • "clear wireless detected-client non-auth" on page 388 • "show wireless wids-security rogue-test-descriptions" on page 378 • "show wireless ap provisioning status" • "wireless device-location start-search"

Revision	*Date*	*Change Description*
		Updated: • “EWS4502/EWS4606 Modules” on page 20 • “Using CLI Help” on page 26 • “show serial” on page 32 • “user” on page 96 • “interface” on page 76 • “ping ipv6” on page 206 • “agetime” on page 216 • “show wireless switch status” on page 229 • “show wireless ap image availability” on page 237 • “show wireless known-client” on page 238 • “show wireless channel-plan history” on page 246 • “show wireless channel-plan proposed” on page 246 • “show wireless power-plan proposed” on page 247 • “security mode” on page 260 • “vap-tun-switch-type” on page 274 • “show wireless network” on page 284 • “accton-ap reset-mode” on page 298 • “show wireless ap profile radio” on page 323 • “clear wireless ap neighbors” on page 337 • “show wireless ap radio status” on page 340 • “show wireless ap rf-scan status” on page 356 • “show wireless client status” on page 361 • “show wireless ssid client status” on page 367 • “show wireless switch client status” on page 368 • “clear wireless detected-client non-auth” on page 388 • “show wireless wids-security rogue-test-descriptions” on page 378 • “show wireless ap provisioning status” • “wireless device-location start-search” **Removed:** • “Email Alerting and Mail Server Commands” • “transport input telnet” • “enable password” • “delete backup” • “ping ipv6 interface” • “country-code method” • “aeroscout” • “rate-limit” • “ap validation” • “redirect mode” • “redirect url” • “wireless ap provision switch” • “wireless ap provision profile” • “clear wireless ap provision”

Revision	Date	Change Description
		• "rate" • "load-balance" • "protection" • "multicast tx-rate" • "agetime ap-provisioning-db"
DCSS Software v1.0.7.1	6/18/2013	Initial release

Additional Documentation

The following documentation provides additional information about EWS4502/EWS4606 software:

- The *EWS4502/EWS4606 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.

About EWS4502/EWS4606 Software

The EWS4502/EWS4606 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

EWS4502/EWS4606 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. EWS4502/ EWS4606 software provides a flexible solution to these ever-increasing needs.

The exact functionality provided by each networking device on which the EWS4502/EWS4606 software base runs varies depending upon the platform and requirements of the EWS4502/EWS4606 software.

EWS4502/EWS4606 software includes a set of comprehensive management functions for managing both EWS4502/EWS4606 software and the network. You can manage the EWS4502/EWS4606 software by using one of the following three methods:

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

Each of the EWS4502/EWS4606 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.

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

EWS4502/EWS4606 software references physical entities such as cards and ports by using a `slot/port` naming convention. The EWS4502/EWS4606 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.

EWS4502/EWS4606 Modules

EWS4502/EWS4606 software consists of flexible modules that can be applied in various combinations of 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 EWS4502/EWS4606 software.

The EWS4502/EWS4606 software suite includes the following modules:

- Switching (Layer 2)
- Wireless
- Quality of Service
- Management (CLI, Web UI, and SNMP)
- IPv6 Management—Allows management of the EWS4502/EWS4606 device 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.

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 EWS4502/EWS4606 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	`EdgeCore Switching>`	Contains a limited set of commands to view basic system information.
Privileged EXEC	`EdgeCore Switching#`	Allows you to issue any `EXEC` command, enter the VLAN mode, or enter the Global Configuration mode.
Global Config	`(EdgeCore Switching) (Config)#`	Groups general setup commands and permits you to make modifications to the running configuration.
VLAN Config	`(EdgeCore Switching) (Vlan)#`	Groups all the VLAN commands.

Interface Config	`(EdgeCore Switching) (Interface` *`slot/port`*`)#`
	
	`(EdgeCore Switching) (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:
		
		`(EdgeCore Switching) (Interface 1/0/1-1/0/4) #`

Line Console	`(EdgeCore Switching) (config-line)#`	Contains commands to configure outbound telnet settings and console interface settings, as well as to configure console login/enable authentication.
Line SSH	`(EdgeCore Switching) (config-ssh)#`	Contains commands to configure SSH login/ enable authentication.
Line Telnet	`(EdgeCore Switching) (config-telnet)#`	Contains commands to configure telnet login/ enable authentication.
Mail Server Config	`(EdgeCore Switching) (Mail-Server)#`	Allows configuration of the email server.

Table 5: CLI Command Modes (Cont.)

Command Mode	*Prompt*	*Mode Description*
Wireless Config Mode	`(EdgeCore Switching) (Config-wireless)#`	Contains global WLAN switch configuration commands and provides access to other WLAN command modes.
AP Config Mode	`(EdgeCore Switching) (Config-ap)#`	Contains commands to configure entries in the local AP database, which is used for AP validation.
AP Profile Config Mode	`(EdgeCore Switching) (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	`(EdgeCore Switching) (Config-ap-profile-radio)#`	Contains commands to modify the radio configuration parameters for an AP profile.
AP Profile VAP Config Mode	`(EdgeCore Switching) (Config-ap-profile-vap)#`	Contains commands to configure radio 1 or radio 2 within an AP profile.
Network Config Mode	`(EdgeCore Switching) (Config-network)#`	Contains commands to configure WLAN settings for up to 64 different networks.
Captive Portal Config Mode	`(EdgeCore Switching) (Config-CP)#`	Contains commands to configure global captive portal settings.
Captive Portal Instance Mode	`(EdgeCore Switching) (Config-CP 1)#`	Contains commands to configure a captive portal instance.
Captive Portal Locale Config Mode	`(EdgeCore Switching) (Config-CP 1 1)#`	Contains commands to configure a captive portal Authentication page, Welcome page, Logout page, and Success page.
Captive Portal Encoded Image Mode	(EdgeCore Switching) (Config-CP-EI)#	Contains commands to configure a captive portal's decoded image size for the page background, branding, and account graphics, as well as the encoded text size.
Device Location Building Config Mode	`(EdgeCore Switching) (Config-building)#`	Contains commands to specify the location of a WLAN device.
Device Location Floor Config Mode	`(EdgeCore Switching) (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`.

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

Command Mode	*Access Method*	*Exit or Access Previous Mode*
Interface Config	From the Global Config mode, enter: `interface slot/port` or `interface` *slot/port*`(startrange)-`*slot/port*`(endrange)`	To exit to the Global Config mode, enter `exit`. To return to the Privileged EXEC mode, enter `Ctrl-Z`.
Line Console	From the Global Config mode, enter `line console`.	To exit to the Global Config mode, enter `exit`. To return to the Privileged EXEC mode, enter `Ctrl-Z`.
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`.
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`.
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`.
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`.
Captive Portal Locale Config Mode	From the Captive Portal Instance mode, enter `locale` *local-id* where *local-id* is the captive portal locale ID.	To exit to the Captive Portal Locale Config mode, enter `exit`. To return to the User EXEC mode, enter `Ctrl-Z`.
Captive Portal Encoded Image Mode	From the Captive Portal Config mode, enter `encoded-image`	To exit to the Captive Portal Encoded Image 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*
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.
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.

```
(EdgeCore Switching) >?

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

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

```
(EdgeCore Switching) #network ?

ipv6                    Configure IPv6 parameters for system network.
javamode                Enable/Disable.
mac-address             Configure MAC Address.
mac-type                Select the locally administered or burned in MAC
                        address.
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.

```
(EdgeCore Switching) #network parms ?

<ipaddr>                Enter the IP address.
none                    Reset IP address and gateway on management interface
```

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

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

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

```
(EdgeCore Switching) #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 28.

Section 2: Management Commands

This chapter describes the management commands available in the EWS4502/EWS4606 CLI.

The Management Commands chapter contains the following sections:

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 171.

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

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.

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

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

```
(admin) #show network

Interface Status.............................. Up
IP Address.................................... 192.168.1.1
Subnet Mask................................... 255.255.255.0
Default Gateway............................... 192.168.1.254
IPv6 Administrative Mode...................... Enabled
IPv6 Prefix is................................ fe80::7272:cfff:fe91:453a/64
Burned In MAC Address......................... 70:72:CF:91:45:3A
Locally Administered MAC address.............. 00:00:00:00:00:00
MAC Address Type.............................. Burned In
Configured IPv4 Protocol...................... None
Configured IPv6 Protocol...................... None
IPv6 AutoConfig Mode.......................... Disabled
Management VLAN ID............................ 1
```

Console Port Access Commands

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

configure

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

Format `configure`

Mode Privileged EXEC

line

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

Format `line {console | telnet | ssh}`

Mode Global Config

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

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

```
(EdgeCore Switching)(config)#line telnet
(EdgeCore Switching)(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	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.

telnet

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

Format `telnet ip-address|hostname port [debug] [line] [localecho]`

Modes Privileged EXEC
User EXEC

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 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.

Term	*Definition*
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.

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

User Account Commands

This section describes the commands you use to add, manage, and delete system users. EWS4502/EWS4606 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.

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.

```
(EdgeCore Switching)(config)# line console
(EdgeCore Switching)(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`* `password` *`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.

```
(EdgeCore Switching) (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.

```
(EdgeCore Switching) (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.

```
(EdgeCore Switching) #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.

```
(EdgeCore Switching) #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.

```
(EdgeCore Switching) (config)# line console
(EdgeCore Switching) (config-line)# login authentication default
```

no login authentication

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

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.

```
(EdgeCore Switching) (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.

```
(EdgeCore Switching) >password
Enter old password:********
Enter new password:********
Confirm new password:********
```

passwords min-length

Use this command to enforce a minimum password length for local users. The value also applies to the enable password. The valid range is 0–64.

Default 8

Format `passwords min-length *0–64*`

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 strength-check

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

Format `no passwords strength-check`

Mode Global Config

passwords strength 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 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 Aging	Length in days that a password is valid.
Password History	Number of passwords to store for reuse prevention.
Lockout Attempts	Number of failed password login attempts before lockout.
Password Strength Check	Shows if the password strength check is enabled.
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.

Term	*Definition*
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

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.

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 61.

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 56.

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 59.

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 59.

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 59.

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.

Term	*Definition*
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. Configure which traps the switch should generate by enabling or disabling the trap condition. If a trap condition is enabled and the condition is detected, the SNMP agent on the switch sends the trap to all enabled trap receivers. You do not have to reset the switch to implement the changes. Cold and warm start traps are always generated and cannot be disabled.

Format `show trapflags`

Mode Privileged EXEC

Term	*Definition*
Authentication Flag	Can be enabled or disabled. The factory default is enabled. Indicates whether authentication failure traps will be sent.
Link Up/Down Flag	Can be enabled or disabled. The factory default is enabled. Indicates whether link status traps will be sent.
Multiple Users Flag	Can be enabled or disabled. The factory default is enabled. Indicates whether a trap will be sent when the same user ID is logged into the switch more than once at the same time (either through Telnet or the serial port).
Spanning Tree Flag	Can be enabled or disabled. The factory default is enabled. Indicates whether spanning tree traps are sent.
ACL Traps	May be enabled or disabled. The factory default is disabled. Indicates whether ACL traps are sent.
Global Wireless Trap Flag	Can be enabled or disabled. The factory default is enabled. Shows if the SNMP agent on the switch is enabled to send traps to the SNMP manager on your network.
Captive Portal Flag	Can be enabled or disabled. The factory default is disabled. Shows if SNMP traps are enabled to be sent from the Captive Portal.

Captive Portal Commands

This section describes the commands you use to configure the captive portal on the switch. You can configure the switch to force an HTTP client on the wireless network to access a special web page (usually for authentication purposes) before gaining normal access to the Internet.

accept-msg

Use this command to configure the text to display when the user does not accept the acceptance use policy. This message displays after the user clicks the button to connect to the network.

The message text must use UTF-16 (16-bit Unicode Transformation Format) character encoding which is capable of encoding all 1,112,064 possible characters in Unicode. For the formal definition of UTFs see Section 3.9, Unicode Encoding Forms in The Unicode Standard. For more information on encoding forms see UTR #17: Unicode Character Encoding Model. Several free UTF conversion tools are available on the web, such as http://http://rishida.net/tools/conversion/.

A sample is shown here:
Display Text: Error: You must acknowledge the Acceptance Use Policy before connecting!
UTF-16: 45 72 72 6F 72 3A 20 59 6F 75 20 6D 75 73 74 AC 6B 6E 6F 77 6C 65 64 67 65 20 74 68 65 ACCE 70 74 61 6E 63 65 20 55 73 65 20 50 6F 6C 69 63 79 BEF 6F 72 65 C 6F 6E 6E 65 63 74 69 6E 67 21

Default Error: You must acknowledge the Acceptance Use Policy before connecting!

Format accept-msg *<UTF-16>*

Mode Captive Portal Locale Configuration

no accept-msg

Use this command to restore the default text to display when the user did not accept the acceptance use policy. This message displays after the user clicks the button to connect to the network.

Format no accept-msg

Mode Captive Portal Locale Configuration

accept-text

Use this command to configure the text to display, which further identifies the network to be accessed by the CP user. This message displays on the Welcome Page under the Welcome Title.

Default You are now authorized and connected to the network.

Format accept-text *<UTF-16>*

Mode Captive Portal Locale Configuration

no accept-text

Use this command to restore the default text to display, which further identifies the network to be accessed by the CP user. This message displays on the Welcome Page under the Welcome Title.

Format no accept-text

Mode Captive Portal Locale Configuration

account-image

Use this command to configure the image name used for the authentication page. This image will display on the captive portal page above the login field. The image display area is 55H x 310W pixels. Your image will be resized to fit the display area.

Default login_key.jpg

Format account-image *<image-name>*

Mode Captive Portal Locale Configuration

no account-image

Use this command to restore the default image used for the authentication page. This image will display on the captive portal page above the login field.

Format no account-image

Mode Captive Portal Locale Configuration

account-label

Use this command to configure the label name for accounting identification. This text is displayed in the Account Title field, and briefly instructs the users to authenticate.

Default Enter your Username.

Format account-label *<UTF-16>*

Mode Captive Portal Locale Configuration

no account-label

Use this command to restore the label name for accounting identification to the default settings. This text is displayed in the Account Title field, and briefly instructs the users to authenticate.

Default None

Format no account-label

Mode Captive Portal Locale Configuration

aup-text

Use this command to enter the text to display in the Acceptance Use Policy field (Authentication page). The acceptance use policy instructs users about the conditions under which they are allowed to access the network. The policy can contain up to 8192 text characters.

Default Acceptance Use Policy

Format aup-text *<UTF-16>*

Mode Captive Portal Locale Configuration

no aup-text

Use this command to restore the text displayed in the Acceptance Use Policy field (Authentication page) to the default setting. The acceptance use policy instructs users about the conditions under which they are allowed to access the network. The policy can contain up to 8192 text characters.

Format no aup-text

Mode Captive Portal Locale Configuration

authentication timeout

To access the network through a portal, the wireless client must first enter authentication information on an authentication Web page. This command specifies the number of seconds to keep the authentication session open with the client. The valid range is 60–600 seconds. When the timeout expires, the switch disconnects any active TCP or SSL connection with the client.

Default 300 seconds

Format `authentication timeout` *`60-600`*

Mode Captive Portal

no authentication timeout

This command resets the authentication timeout to the default setting.

Default 300 seconds

Format `no authentication timeout`

Mode Captive Portal

background-color

Use this command to set the background color for the Captive Port Authentication page. Enter the name of a well known color e.g., “red” or the hexadecimal code e.g, #FF0000. The valid range of colors is #000000 through #FFFFFF.

Default `#BFBFBF, gray75`

Format `background-color {`*`color-name`* | *`#000000-#FFFFFF`*`}`

Mode Captive Portal Configuration

no background-color

Use this command to reset the background color for the Captive Port Authentication page to default color.

Format `no background-color`

Mode Captive Portal Configuration

background-image

Use this command to configure the file name for background image used on the Authentication page.

Default cp_bkg.jpg

Format background-image *image-name*

Mode Captive Portal Locale Configuration

no background-image

Use this command to restore the file name for background image used on the Authentication page to the default setting.

Format no background-image

Mode Captive Portal Locale Configuration

block

Use this command to block authentication attempts on the captive portal configuration instance. If the CP is blocked, users cannot gain access to the network through the CP. Use this function to temporarily protect the network during unexpected events, such as denial of service attacks. This function is only available when the operational status for the CP is enabled.

Default `unblocked`

Format block

Mode Captive Portal Configuration

unblock

Use this command to unblock authentication attempts on the captive portal configuration instance.

Format unblock

Mode Captive Portal Configuration

branding-image

Use this command to select the name of the image file to display on the top left corner of the Authentication page, Welcome page, and Logout Success page. This image is used for branding purposes, such as the company logo.

Default ec_logo.jpg

Format branding-image *image-name*

Mode Captive Portal Locale Configuration

no branding-image

Use this command to restore the name of the image file to display on the top left corner of the Authentication page, Welcome page, and Logout Success page to the default setting. This image is used for branding purposes, such as the company logo.

Format no branding-image

Mode Captive Portal Locale Configuration

browser-title

Use this command to enter the text to display on the client's Web browser title bar or tab.

Default Captive Portal

Format browser-title *<UTF-16>*

Mode Captive Portal Locale Configuration

no browser-title

Use this command to restore the text to display on the client's Web browser title bar or tab to the default setting.

Format no browser-title

Mode Captive Portal Locale Configuration

button-label

Use this command to enter the text to display on the button the user clicks to connect to the network.

Default Connect

Format button-label *<UTF-16>*

Mode Captive Portal Locale Configuration

no button-label

Use this command to restore the text to display on the button the user clicks to connect to the network.

Format no button-label

Mode Captive Portal Locale Configuration

captive-portal

This command enters captive portal configuration mode.

Format `captive-portal`

Mode Global Config

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

```
(EdgeCore Switching) (Config)#captive-portal

(EdgeCore Switching) (Config-CP)#
```

captive-portal client deauthenticate

This command forces the captive portal to disconnect authenticated clients. When no parameters are supplied, the AC deauthenticates all clients from all captive portal. Enter a MAC address to deauthenticast a specific client, or enter a specific captive portal instance to disconnect all clients from that captive portal.

Format `captive-portal client deauthenticate [1-10 | macaddr]`

Mode Privileged EXEC

Parameter	*Definition*
1-10	A captive portal configuration instance.
macaddr	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`.

clear

Use this command to set all configuration settings will be set to the default values for this CP configuration instance.

Format clear

Mode Captive Portal Configuration

code

Use this command to enter locale code typically recognized by Internet browsers. This codes can be found on various sites, such as http://www.metamodpro.com/browser-language-codes.

Default en

Format code <*locale-code*>

Mode Captive Portal Locale Configuration

no code

Use this command to restore the default locale code.

Format no code

Mode Captive Portal Locale Configuration

configuration

Use this command to enter Captive Portal Configuration mode for a specific instance.

Format `configuration 1-10`

Mode Captive Portal

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

```
(EdgeCore Switching) (Config-CP)#configuration 1

(EdgeCore Switching) (Config-CP 1)#
```

decoded-image-size

Use this command to configure the decoded image size of the page background, branding, and account graphics. The valid range is 0 to 3072000 KB. However, for the related images to fit together well, the image should be 5KB maximum, 200x200 pixels, GIF or JPG format.

Format `decoded-image-size` *`0-3072000`*

Mode Captive Portal Encoded Image

no decoded-image-size

Use this command to reset the decoded image size of the page background, branding, and account graphics to the default size.

Format `no decoded-image-size`

Mode Captive Portal Encoded Image

denied-msg

Use this command to enter the text to display when the user does not provide valid authentication information. This message displays after the user clicks the button to connect to the network.

Default Error: Invalid Credentials, please try again!

Format denied-msg *<UTF-16>*

Mode Captive Portal Locale Configuration

no denied-msg

Use this command to restore the text displayed when the user does not provide valid authentication information to the default setting. This message displays after the user clicks the button to connect to the network.

Format denied-msg *<UTF-16>*

Mode Captive Portal Locale Configuration

enable (Captive Portal)

Use this command to enable the CP feature on the switch.

Format `enable`

Mode Captive Portal

no enable

Use this command to disable the CP feature on the switch.

Format `no enable`

Mode Captive Portal

enable (Captive Portal Configuration)

Use this command to enable the captive portal configuration instance.

Format enable

Mode Captive Portal Configuration

no enable

Use this command to disable the captive portal configuration instance.

Format disable

Mode Captive Portal Configuration

encoded-image

Use this command to enter CP encoded image mode. This mode is used to configure the decoded image size or the encoded text size used for the CP Welcome page.

Format `encoded-image`

Mode Captive Portal

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

```
(EdgeCore Switching) (Config-CP)#encoded-image

(EdgeCore Switching) (Config-CP-EI)# ?

decoded-image-size       Configure Captive Portal decoded image size.
encoded-image-text       Configure Captive Portal encoded image text.
exit                     To exit from the mode.
```

no encoded-image

Use this command to remove the CP encoded image.

Format `encoded-image`

Mode Captive Portal

encoded-image-text

Use this command to configure the encoded text. The valid range is 0 to 256 characters.

no encoded-image-text

Use this command to reset the encoded text.

Format `no encoded-image-text`

Mode Captive Portal Encoded Image

ext-redirect

Use this command to specify that the CP should redirect the newly authenticated client to the configured URL.

Default Disabled

Format ext-redirect

Mode Captive Portal Configuration

no ext-redirect

Use this command to stop the CP from redirecting the newly authenticated client to the configured URL. If this option is selected, the user sees the locale-specific welcome page after a successful verification.

Format no ext-redirect

Mode Captive Portal Configuration

ext-redirect-url

Use this command to specify the URL to which the newly authenticated client is redirected if the URL redirect mode (i.e., ext-redirect command) is enabled.

Default None

Format ext-redirect-url *url*

Mode Captive Portal Configuration

font-list

Use this command to configure preferred fonts for this locale. The specified fonts will be used for all text displayed on the CP page. Use a comma to separate each font in the list.

Default arial, sans-serif

Format font-list *font,font*,...

Mode Captive Portal Locale Configuration

no font-list

Use this command to restore the default fonts used for this locale.

Format no font-list

Mode Captive Portal Locale Configuration

foreground-color

Use this command to set the foreground color for the Captive PortAuthentication page. Enter the name of a well known color e.g., “red” or the hexadecimal code e.g, #FF0000. The valid range of colors is #000000 through #FFFFFF.

Default `#999999, gray6`

Format `foreground-color {`*`color-name`* | *`#000000-#FFFFFF`*`}`

Mode Captive Portal Configuration

no foreground-color

Use this command to reset the foreground color for the Captive PortAuthentication page to default color.

Format `no foreground-color`

Mode Captive Portal Configuration

group

If the verification mode is set to Local or RADIUS by the verification command), use the **group** command to assign an existing user group to the captive portal instance or to create a new group. All users who belong to the group are permitted to access the network through this portal. The user group list is the same for all CP configuration instances on the switch.

Format group *1-10*

Mode Captive Portal Configuration

no group

If the verification mode is set to Local or RADIUS by the verification command), use the **no group** command to disassociate an existing user group from the captive portal instance. All users who belong to the group are denied access the network through this portal.

Format group *1-1-0*

Mode Captive Portal Configuration

http

Use this command to configure a specific TCP port for HTTP traffic. HTTP traffic uses port 80, but you can set this port to any number between 0-65535 (excluding ports 80, 443, and the configured switch management port). If you change the HTTP port number for the captive portal to anything other than 80, all Web addresses entered by a wireless client must include the port number. For example: http://sample:8000/documents/.

Default 80

Format `http 0-65535`

Mode Captive Portal

no http

Use this command to reset the TCP port for HTTP traffic to port 80.

Format `no http`

Mode Captive Portal

https

Use this command to configure a specific TCP port for HTTP traffic over SSL (HTTPS). HTTPS traffic uses port 443, but you can set this port to any number between 0-65535 (excluding ports 80, 443, and the configured switch management port). If you change the HTTPS port number for the captive portal to anything other than 443, all Web addresses entered by a wireless client must include the port number. For example: https://sample:8000/documents/.

Default 443

Format `http 0-65535`

Mode Captive Portal

no https

Use this command to reset the TCP port for HTTPS traffic to port 443.

Format `no http`

Mode Captive Portal

idle-timeout

Use this command to configure the number of seconds a user can remain idle before being automatically logged out. If the value is set to 0 then the timeout is not enforced.

Default 900 seconds

Format idle-timeout *0-900*

Mode Captive Portal Configuration

no idle-timeout

Use this command to reset the number of seconds a user can remain idle before being automatically logged out to the default value.

Default 900 seconds

Format no idle-timeout

Mode Captive Portal Configuration

instructional-text

Use this command to enter text describing how to perform authentication on the Captive Portal.

Default To start using this service, enter your credentials and click the Connect button.

Format instructional-text *<UTF-16>*

Mode Captive Portal Locale Configuration

no instructional-text

Use this command to restore the text describing how to perform authentication on the Captive Portal to the default setting.

Format no instructional-text

Mode Captive Portal Locale Configuration

interface

Use this command to associate a configured captive portal instance with a specific physical interface. The CP feature only runs on the wired or wireless interfaces that you specify. A CP can have multiple interfaces associated with it, but an interface can be associated to only one CP at a time.

Note: When associating a physical (wired) interface with a captive portal configuration, note the following restrictions:

- Captive portal and STP should not be enabled on the same physical interface.
- Captive portal and 802.1X cannot be enabled on the same physical interface.
- Port security and captive portal cannot be enabled on the same physical interface.
- If a physical interface is made a LAG member, the captive portal becomes disabled on the interface.

Format interface *<slot/port>*

Mode Captive Portal Configuration

no interface

Use this command to disassociate a configured captive portal instance from an specific physical interface.

Format no interface *<slot/port>*

Mode Captive Portal Configuration

link

Use this command to configure locale link text for identity and language selection. The default text depends on the selected language.

Format link *<UTF-16>*

Mode Captive Portal Locale Configuration

no link

Use this command to restore the default locale link text for identity and language selection.

Format no link

Mode Captive Portal Locale Configuration

locale

Use this command to enter captive portal configuration locale mode. Up to five different locales may be configured.

Format locale *1-5*

Mode Captive Portal Configuration

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

```
(EdgeCore Switching) (Config-CP 1)#locale 1

(EdgeCore Switching) (Config-CP 1 1)#?
```

logout-browser-title

Use this command to enter the text to display on the title bar of the Logout page.

Default Captive Portal - Logout

Format logout-browser-title *<UTF-16>*

Mode Captive Portal Locale Configuration

no logout-browser-title

Use this command to restore the default text displayed on the title bar of the Logout page.

Format no logout-browser-titl

Mode Captive Portal Locale Configuration

logout-button-label

Use this command to configure text for the logout button.

Default Logout

Format logout-button-label *<UTF-16>*

Mode Captive Portal Locale Configuration

no logout-button-label

Use this command to restore the default text for the logout button.

Format no logout-button-label

Mode Captive Portal Locale Configuration

logout-confirmation-text

Use this command to configure the logout confirmation text.

Default Are you sure you want to logout?

Format logout-confirmation-text *<UTF-16>*

Mode Captive Portal Locale Configuration

no logout-confirmation-text

Use this command to restore the default logout confirmation text.

Format no logout-confirmation-text

Mode Captive Portal Locale Configuration

logout-success-background-image

Use this command to configure the file used for background image.

Default cp_bkg.png

Format logout-success-background-image *<image-name>*

Mode Captive Portal Locale Configuration

no logout-success-background-image

Use this command to restore the default file used for background image.

Format no logout-success-background-image

Mode Captive Portal Locale Configuration

logout-success-browser-title

Use this command to enter the text to display on the title bar of the Logout Success page.

Default Captive Portal – Logged Out

Format logout-success-browser-title *<UTF-16>*

Mode Captive Portal Locale Configuration

no logout-success-browser-title

Use this command to restore the default text to display on the title bar of the Logout Success page.

Format no logout-success-browser-title

Mode Captive Portal Locale Configuration

logout-success-text

Use this command to configure the text to display confirming that the user has been successfully logged out.

Default You have successfully logged out.

Format logout-success-text *<UTF-16>*

Mode Captive Portal Locale Configuration

no logout-success-text

Use this command to restore the default text displayed confirming that the user has been successfully logged out.

Format no logout-success-text

Mode Captive Portal Locale Configuration

logout-success-title

Use this command to configure text used for logout success title. This is the text that identifies the page.

Default Logout Success!

Format logout-success-title *<UTF-16>*

Mode Captive Portal Locale Configuration

no logout-success-title

Use this command to restore the default text used for logout success title. This is the text that identifies the page.

Format no logout-success-title

Mode Captive Portal Locale Configuration

logout-text

Use this command to configure text for logout instructions.

Default You are now authorized and connected to the network. Please retain this small logout window in order to de-authenticate. Press the logout button when done.

Format logout-text *<UTF-16>*

Mode Captive Portal Locale Configuration

no logout-text

Use this command to restore the default text used for logout instructions.

Format logout-text *<UTF-16>*

Mode Captive Portal Locale Configuration

logout-title

Use this command to enter the text to use as the page title.

Default Web Authentication

Format logout-title *<UTF-16>*

Mode Captive Portal Locale Configuration

no logout-title

Use this command to restore the default text to use as the page title.

Format no logout-title

Mode Captive Portal Locale Configuration

max-bandwidth-down

Use this command to configure the maximum speed, in bytes per second, that a client can receive traffic when using the captive portal. This setting limits the bandwidth at which the client can receive data from the network. Setting the rate to 0 means that the download bandwidth is unlimited.

Default 0

Format max-bandwidth-down *0-536870911*

Mode Captive Portal Configuration

no max-bandwidth-down

Use this command to restore the default maximum speed, in bytes per second, that a client can receive traffic when using the captive portal.

Format no max-bandwidth-down

Mode Captive Portal Configuration

max-bandwidth-up

Use this command to configure the maximum speed, in bytes per second, that a client can transmit traffic when using the captive portal. This setting limits the bandwidth at which the client can send data into the network. Setting the rate to 0 means that the upload bandwidth is unlimited.

Default 0

Format max-bandwidth-up *0-536870911*

Mode Captive Portal Configuration

no max-bandwidth-up

Use this command to restore the default maximum speed, in bytes per second, that a client can transmit traffic when using the captive portal.

Format no max-bandwidth-up

Mode Captive Portal Configuration

max-input-octets

Use this command to configure the maximum number of bytes that a client is allowed to receive when using the captive portal. After this limit has been reached the user will be disconnected. Setting this parameter to 0 means that the maximum number of bytes that can be received is unlimited.

Default 0

Format max-input-octets *0-4294967295*

Mode Captive Portal Configuration

no max-input-octets

Use this command to restore the default maximum number of bytes that a client is allowed to receive when using the captive portal.

Format no max-input-octets

Mode Captive Portal Configuration

max-output-octets

Use this command to configure the maximum number of bytes that a client is allowed to transmit when using the captive portal. After this limit has been reached the user will be disconnected. Setting this parameter to 0 means that the maximum number of bytes that can be transmitted is unlimited.

Default 0

Format max-output-octets *0-4294967295*

Mode Captive Portal Configuration

no max-output-octets

Use this command to restore the default maximum number of bytes that a client is allowed to transmit when using the captive portal.

Format no max-output-octets

Mode Captive Portal Configuration

max-total-octets

Use this command to configure the maximum number of bytes the user is allowed to transfer (sum of bytes transmitted and received). After this limit has been reached the user will be disconnected. Setting this parameter to 0 means that the maximum number of bytes that can be transmitted and received is unlimited.

Default 0

Format max-total-octets *0-4294967295*

Mode Captive Portal Configuration

no max-total-octets

Use this command to restore the default maximum number of bytes the user is allowed to transfer (sum of bytes transmitted and received).

Format no max-total-octets

Mode Captive Portal Configuration

name

Use this command to configure the name of this captive portal configuration instance. The name can be up to 32 alphanumeric characters in length.

Default Default

Format name *cp-name*

Mode Captive Portal Configuration

no name

Use this command to restore the default name of this captive portal configuration instance.

Format no name

Mode Captive Portal Configuration

password-label

Use the command to enter the text to display next to the field where the user enters the password.

Default Password

Format password-label <*UTF-16*>

Mode Captive Portal Locale Configuration

no password-label

Use the command to restore the default text to display next to the field where the user enters the password.

Format no password-label

Mode Captive Portal Locale Configuration

popup-text

Use this command to configure text used to remind user to allow popups from our web site.

Default Please allow pop-ups to display the logout WEB page.

Format popup-text <*UTF-16*>

Mode Captive Portal Locale Configuration

no popup-text

Use this command to restore the default text used to remind user to allow popups from our web site.

Format popup-text *<UTF-16>*

Mode Captive Portal Locale Configuration

protocol

Use this command to choose whether to use HTTP or HTTPs as the protocol for the captive portal to use during the verification process.

Default HTTP

Format name *cp-name*

Mode Captive Portal Configuration

no protocol

Use this command to restore the default protocol the captive portal will use during the verification process.

Format name *cp-name*

Mode Captive Portal Configuration

resource-msg

Use this command to enter the text to display when the system has rejected authentication due to system resource limitations. This message may display after the user clicks the button to connect to the network.

Default Error: Limited Resources, please reconnect and try again later!

Format resource-msg *<UTF-16>*

Mode Captive Portal Locale Configuration

no resource-msg

Use this command to restore the default text to display when the system has rejected authentication due to system resource limitations.

Format no resource-msg

Mode Captive Portal Locale Configuration

script-text

Use this command to configure text used to notify user if their browser has javascript disabled.

Default Please enable Javascript to display the logout WEB page.

Format script-text *<UTF-16>*

Mode Captive Portal Locale Configuration

no script-text

Use this command to restore the default text used to notify user if their browser has javascript disabled.

Format no script-text

Mode Captive Portal Locale Configuration

separator-color

Use this command to set the separator color for the Captive PortAuthentication page. Enter the name of a well known color e.g., “red” or the hexadecimal code e.g, #FF0000. The valid range of colors is #000000 through #FFFFFF.

Default `#B70024`

Format `separator-color {`*`color-name`* | *`#000000-#FFFFFF`*`}`

Mode Captive Portal Configuration

no separator-color

Use this command to reset the separator color for the Captive PortAuthentication page to default color.

Format `no separator-color`

Mode Captive Portal Configuration

show captive-portal

This command displays administrative settings for the captive portal function.

Format `show captive-portal`

Mode Privileged EXEC

Term	*Definition*
Administrative Mode	Shows whether the CP is enabled globally for the AC.
Operational Status	Shows the operational status of the CP. If disabled, one of the following reasons is displayed: • None • Administratively Disabled • No IPv4 Address
CP IP Address	Shows the captive portal IP address.

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

```
(EdgeCore Switching) #show captive-portal

Administrative Mode.......................... Enable
Operational Status........................... Enabled
CP IP Address................................ 192.168.0.22e
```

show captive-portal client status

This command displays summary information about all connected clients or detailed information about a client if a MAC address is specified.

Format `show captive-portal client [macaddr] status`

Mode Privileged EXEC

Term	*Definition*
MAC Address	Identifies the MAC address of the wireless client. If the MAC address is marked with an asterisk (*), the authenticated client is authenticated by a peer switch. In order words, the cluster controller was not the authenticator.
IP Address	Identifies the IP address of the wireless client (if applicable).
User Name	Displays the user name (or Guest ID) of the connected client.
Protocol	Shows the current connection protocol, which is either HTTP or HTTPS.
Verify Mode	Shows the current account type, which is Guest, Local, or RADIUS.
Session Time	Shows the amount of time that has passed since the client was authorized
CP ID	The CP configuration ID.
CP Name	CP configuration name.
Interface	Identifies the interface the wireless client is using.
Interface Description	The wireless interfaces that are currently associated with the captive portal the wireless client is using. Wireless interfaces are identified by the wireless network number and SSID.
Session Timeout	The number of seconds to wait before terminating a session.
Switch MAC Address	Shows the MAC address of the switch handling authentication for this client. If clustering is supported, this field might display the MAC address of a peer switch in the cluster.
Switch IP Address	Shows the IP address of the switch handling authentication for this client. If clustering is supported, this field might display the IP address of a peer switch in the cluster.
Switch Type	Shows if the AC to which this client is associated is the local cluster controller or a peer switch.

Example: The following shows an example of the CLI command used to display summary information about all associated clients.

```
(EdgeCore Switching) #show captive-portal client status

      MAC Address                                    Verify
(*)Peer Authenticated   IP Address    User Name  Protocol  Mode  Session Time
--------------------- --------------- ---------- -------- ------ ------------
 74:DA:38:07:BF:CD    192.168.0.2     steve      HTTP     Guest  0d:00:07:25
```

The following shows an example of the CLI command used to display detailed information about a specific client.

```
(EdgeCore Switching) #show captive-portal client 74:da:38:07:bf:cd status

Client MAC Address.............................. 74:DA:38:07:BF:CD
Client IP Address............................... 192.168.0.22
Protocol Mode................................... HTTP
Verification Mode............................... Guest
CP ID........................................... 1
```

```
CP Name..................................... Default
Interface................................... 6/1
Interface Description....................... Wireless Network 1 - GuestNet...
User Name................................... steve
Session Timeout............................. 0d:00:24:37
Switch MAC Address.......................... 70:72:CF:CF:9B:50
Switch IP Address........................... 192.168.0.22
Switch Type................................. Local
```

show captive-portal client statistics

This command displays information about the traffic a client has sent or received.

Format `show captive-portal client macaddr statistics`

Mode Privileged EXEC

Term	*Definition*
Client MAC Address	Identifies the MAC address of the wireless client.
Bytes Received	Total bytes the client has received
Bytes Transmitted	Total bytes the client has transmitted
Packets Received	Total packets the client has received
Packets Transmitted	Total packets the client has transmitted

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

```
(EdgeCore Switching) #show captive-portal client 74:da:38:07:bf:cd statistics

Client MAC Address.......................... 74:DA:38:07:BF:CD
Bytes Received.............................. 621807
Bytes Transmitted........................... 1115404
Packets Received............................ 4599
Packets Transmitted......................... 3895
```

show captive-portal configuration

This command displays configuration settings about the captive portals or associated wireless clients.

Format `show captive-portal configuration {cp-id [client status] | interface [slot/port] | locales | status}] | client status | status}`

Mode Privileged EXEC

Parameter	*Definition*
cp-id	The switch supports 10 CP configuration instances.
client status	Shows information about all authenticated wireless clients that are connected through the captive portal.
interface	Shows information for the interfaces assigned to a captive portal instance.
locales	Shows the configures locale-specific codes for the CP welcome pages.
status	Shows basic configuration settings for CP instances.

Term	*Definition*
CP ID	The switch supports 10 CP configuration instances.
CP Name	The configuration name assigned a CP instance.
Client MAC Address	Identifies the MAC address of the wireless client.
Client IP Address	Identifies the IP address of the wireless client.
Interface	The logical interface which represents a logical slot and port number. For a captive portal instance, where slot number is 6 and the port number is the CP instance.
Mode	Shows whether the CP is enabled.
Protocol	Indicates whether the portal uses HTTP or HTTPS.
Verification	Shows the type of user verification to perform: • Guest - The user does not need to be authenticated by a database. • Local - The switch uses a local database to authenticated users. • RADIUS - The switch uses a database on a remote RADIUS server to authenticate users. • Languages - Shows the number of languages that are configured for this captive portal.
Operational Status	Shows whether the CP feature is globally enabled.
Block Status	Indicates whether the captive portal is temporarily blocked for authentications.
Configured Locales	Shows the number of welcome pages, normally configured for specific languages.
Authenticated Users	Shows the number of users currently authenticated to all captive portal instances on this switch.
Interface Description	Shows the wireless interface associated with each client, identified by the wireless network number and SSID.
Activation Status	Shows whether the portal is active on the specified interface.
User Logout Mode	If enable, an authenticated client can deauthenticate from the network. If this option is not enabled or the user does not specifically request logout, the client connection status remains authenticated until the CP deauthenticates the user, for example by reaching the idle timeout or session timeout values.
URL Redirect Mode	If enabled, the CP will redirect the newly authenticated client to the configured URL. Otherwise, the user sees the locale-specific welcome page after a successful verification.
Session Timeout	Shows the number of seconds to wait before terminating a session. A user is logged out once the session timeout is reached. If the value is set to 0 then the timeout is not enforced. The default value is 3600 (1 hour).
Idle Timeout	Shows the number of seconds a user can remain idle before being automatically logged out. If the value is set to 0 then the timeout is not enforced.The default value is 0.
Max Bandwidth Up (bytes/sec)	Shows the maximum speed, in bytes per second, that a client can transmit traffic when using the captive portal. This setting limits the bandwidth at which the client can send data into the network.
Max Bandwidth Down (bytes/sec)	Shows the maximum speed, in bytes per second, that a client can receive traffic when using the captive portal. This setting limits the bandwidth at which the client can receive data from the network.
Max Input Octets (bytes)	Shows the maximum number of bytes that a client is allowed to receive when using the captive portal. After this limit has been reached the user will be disconnected.
Max Output Octets (bytes)	Shows the maximum number of bytes that a client is allowed to transmit when using the captive portal. After this limit has been reached the user will be disconnected.

Term	*Definition*
Max Total Octets (bytes)	Shows the maximum number of bytes the user is allowed to transfer (sum of bytes transmitted and received). After this limit has been reached the user will be disconnected.

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

```
(EdgeCore Switching) #show captive-portal configuration client status

CP ID        CP Name        Client MAC Address Client IP Address Interface
----- --------------------- ------------------ ----------------- ---------
1     Default               74:DA:38:07:BF:CD  192.168.0.2       6/1

(EdgeCore Switching) #show captive-portal configuration status

CP ID       CP Name         Mode   Protocol Verification
----- -------------------- ------- -------- ------------
1     Default              Enable  HTTP     Guest

(EdgeCore Switching) #show captive-portal configuration 1

CP ID..................................... 1
CP Name................................... Default
Operational Status........................ Enabled
Block Status.............................. Not Blocked
Configured Locales........................ 1
Authenticated Users....................... 1

(EdgeCore Switching) #show captive-portal configuration 1 client status

CP ID..................................... 1
CP Name................................... Default

     Client           Client
   MAC Address      IP Address    Interface        Interface Description
----------------- -------------- --------- ----------------------------------
74:DA:38:07:BF:CD 192.168.0.2     6/1       Wireless Network 1 - GuestNetwork

(EdgeCore Switching) #show captive-portal configuration 1 interface

CP ID..................................... 1
CP Name................................... Default

                                                 Activation    Block
Interface        Interface Description             Status      Status
--------- ---------------------------------------- ------------ -----------
6/1       Wireless Network 1 - GuestNetwork        Enabled      Not Blocked

(EdgeCore Switching) #show captive-portal configuration 1 locales

Locale Code
---------------
en

(EdgeCore Switching) #show captive-portal configuration 1 status

CP ID..................................... 1
CP Name................................... Default
```

```
CP Mode..................................... Enable
Protocol Mode............................... HTTP
Verification Mode........................... Guest
User Logout Mode............................ Disable
URL Redirect Mode........................... Disable
Session Timeout............................. 3600
Idle Timeout................................ 0
Max Bandwidth Up (bytes/sec)................ 0
Max Bandwidth Down (bytes/sec).............. 0
Max Input Octets (bytes).................... 0
Max Output Octets (bytes)................... 0
Max Total Octets (bytes).................... 0
```

show captive-portal interface client status

This command displays information about a wireless client associated with a specified captive portal instance, or about all wireless clients associated with every captive port instance if no instance is specified.

Format `show captive-portal interface [slot/port] client status`

Mode Privileged EXEC

Term	*Definition*
Interface	The logical interface which represents a logical slot and port number. For a captive portal instance, where slot number is 6 and the port number is the CP instance.
Interface Description	The wireless interfaces that are currently associated with the captive portal the wireless client is using. Wireless interfaces are identified by the wireless network number and SSID.
Client MAC Address	Identifies the MAC address of the wireless client.
Client IP Address	Identifies the IP address of the wireless client.
CP ID	The switch supports 10 CP configuration instances.
CP Name	The configuration name assigned a CP instance.
Protocol Verification	Shows the type of user verification to perform: • Guest - The user does not need to be authenticated by a database. • Local - The switch uses a local database to authenticated users. • RADIUS - The switch uses a database on a remote RADIUS server to authenticate users. • Languages - Shows the number of languages that are configured for this captive portal.

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

```
(EdgeCore Switching) #show captive-portal interface client status

                                                    Client          Client
Interface        Interface Description            MAC Address      IP Address
--------- ---------------------------------- ----------------- ---------------
6/1       Wireless Network 1 - GuestNetwork   00:25:D3:8F:F9:95 192.168.0.102
6/2       Wireless Network 2 - ManagedSSID_2
6/3       Wireless Network 3 - ManagedSSID_3
6/4       Wireless Network 4 - ManagedSSID_4
6/5       Wireless Network 5 - ManagedSSID_5
6/6       Wireless Network 6 - ManagedSSID_6
```

```
6/7       Wireless Network 7 - ManagedSSID_7
6/8       Wireless Network 8 - ManagedSSID_8
6/9       Wireless Network 9 - ManagedSSID_9
6/10      Wireless Network 10 - ManagedSSI...
6/11      Wireless Network 11 - ManagedSSI...
6/12      Wireless Network 12 - ManagedSSI...
6/13      Wireless Network 13 - ManagedSSI...
6/14      Wireless Network 14 - ManagedSSI...
6/15      Wireless Network 15 - ManagedSSI...
6/16      Wireless Network 16 - ManagedSSI...

(EdgeCore Switching) #show captive-portal interface 6/1 client status
Interface..................................... 6/1
Interface Description......................... Wireless Network 1 - GuestNet...

     Client           Client
   MAC Address      IP Address    CP ID      CP Name      Protocol Verification
----------------- --------------- ----- ----------------- -------- ------------
00:25:D3:8F:F9:95 192.168.0.102   1     Default           HTTP     Guest
```

show captive-portal interface capability

This command displays a summary of the client capability for all interfaces, or a detailed list of client capability for a specified CP instance.

Format `show captive-portal interface capability [slot/port]`

Mode Privileged EXEC

Term	*Definition*
Interface	The logical interface which represents a logical slot and port number. For a captive portal instance, where slot number is 6 and the port number is the CP instance.
Interface Description	The wireless interfaces that are currently associated with the captive portal the wireless client is using. Wireless interfaces are identified by the wireless network number and SSID.
Interface Type	Shows the interface type as wireless.
Session Timeout	Shows that session timout is supported.
Idle Timeout	Shows that idle timeout is supported.
Bytes Received Counter	Shows that the bytes received counter is supported.
Bytes Transmitted Counter	Shows that the bytes transmitted counter is supported.
Packets Received Counter	Shows that the packets received counter is supported.
Packets Transmitted Counter	Shows that the packets transmitted counter is supported.
Roaming	Shows that wireless client roaming among access points managed by the AC is supported

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

```
(EdgeCore Switching) #show captive-portal interface capability

Interface        Interface Description                Type
---------  ------------------------------------- ----------
6/1        Wireless Network 1 - GuestNetwork        Wireless
6/2        Wireless Network 2 - ManagedSSID_2       Wireless
6/3        Wireless Network 3 - ManagedSSID_3       Wireless
6/4        Wireless Network 4 - ManagedSSID_4       Wireless
6/5        Wireless Network 5 - ManagedSSID_5       Wireless
6/6        Wireless Network 6 - ManagedSSID_6       Wireless
6/7        Wireless Network 7 - ManagedSSID_7       Wireless
6/8        Wireless Network 8 - ManagedSSID_8       Wireless
6/9        Wireless Network 9 - ManagedSSID_9       Wireless
6/10       Wireless Network 10 - ManagedSSID_10     Wireless
6/11       Wireless Network 11 - ManagedSSID_11     Wireless
6/12       Wireless Network 12 - ManagedSSID_12     Wireless
6/13       Wireless Network 13 - ManagedSSID_13     Wireless
6/14       Wireless Network 14 - ManagedSSID_14     Wireless
6/15       Wireless Network 15 - ManagedSSID_15     Wireless
6/16       Wireless Network 16 - ManagedSSID_16     Wireless

(EdgeCore Switching) #show captive-portal interface capability 6/1

Interface..................................... 6/1
Interface Description......................... Wireless Network 1 - GuestNet...
Interface Type................................ Wireless
Session Timeout............................... Supported
Idle Timeout.................................. Supported
Bytes Received Counter........................ Supported
Bytes Transmitted Counter..................... Supported
Packets Received Counter...................... Supported
Packets Transmitted Counter................... Supported
Roaming....................................... Supported
```

show captive-portal interface configuration status

This command displays information for the configuration status all captive portal configuration instances or for a specified instance.

Format `show captive-portal interface configuration [cp-id] status}`

Mode Privileged EXEC

Term	*Definition*
CP ID	The switch supports 10 CP configuration instances.
CP Name	The configuration name assigned a CP instance.
Interface	The logical interface which represents a logical slot and port number. For a captive portal instance, where slot number is 6 and the port number is the CP instance.
Interface Description	The wireless interfaces that are currently associated with the captive portal the wireless client is using. Wireless interfaces are identified by the wireless network number and SSID.
Interface Type	Shows the interface type as wireless.

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

```
(EdgeCore Switching) #show captive-portal interface configuration status

CP ID      CP Name       Interface        Interface Description          Type
----- ------------------ --------- ---------------------------------- --------
1     Default            6/1       Wireless Network 1 - GuestNetwork   Wireless
2     TPS                6/2       Wireless Network 2 - ManagedSSID_2  Wireless

(EdgeCore Switching) #show captive-portal interface configuration 1 status

CP ID..................................... 1
CP Name................................... Default

Interface        Interface Description          Type
--------- ---------------------------------- --------
6/1       Wireless Network 1 - GuestNetwork   Wireless
```

show captive-portal status

This command displays information for the global configuration status for all captive portal configuration instances.

Format `show captive-portal status`

Mode Privileged EXEC

Term	*Definition*
Additional HTTP Port	HTTP traffic uses port 80, but you can configure an additional port for HTTP traffic. Port number can range between 0-65535 (excluding ports 80, 443, and the configured switch management port).
Additional HTTP Secure Port	HTTP traffic over SSL (HTTPS) uses port 443, but you can configure an additional port for HTTPS traffic. Port number can range between 0-65535 (excluding ports 80, 443, and the configured switch management port).
Peer Switch Statistics Reporting Interval	The interval at which peer switches report statistics on wireless clients associated with a captive portal.
Authentication Timeout	To access the network through a portal, the wireless client must first enter authentication information on an authentication Web page. This timeout is number of seconds to keep the authentication session open with the client. When the timeout expires, the switch disconnects any active TCP or SSL connection with the client.
Supported Captive Portals	Shows the number of supported captive portals in the system.
Active Captive Portals	Shows the number of captive portal instances that are operationally enabled.
Local Supported Users	Shows the number of entries that the Local User database supports.
Configured Local Users	Shows the number of manually configured local users.
System Supported Users	Shows the number of authenticated users that the system can support.
Authenticated Users	Shows the number of users currently authenticated to all captive portal instances on this switch.

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

```
(EdgeCore Switching) #show captive-portal status

Additional HTTP Port..........................  0
Additional HTTP Secure Port...................  0
Peer Switch Statistics Reporting Interval......  120
Authentication Timeout........................  300
Supported Captive Portals.....................  10
Configured Captive Portals....................  2
Active Captive Portals........................  2
Local Supported Users.........................  8192
Configured Local Users........................  0
System Supported Users........................  1024
Authenticated Users...........................  1
```

show captive-portal trapflags

This command displays whether or not SNMP traps are sent from the Captive Portal and the captive portal events that will generate a trap. Note that captive portal traps can be sent only if the captive portal trap mode is enabled.

Format `show captive-portal status`

Mode Privileged EXEC

Term	*Definition*
Client Authentication Failure Traps	Shows if the SNMP agent sends a trap when a client attempts to authenticate with a captive portal but is unsuccessful.
Client Connection Traps	Shows if the SNMP agent sends a trap when a client authenticates with and connects to a captive portal.
Client Database Full Traps	Shows if the SNMP agent sends a trap each time an entry cannot be added to the client database because it is full.
Client Disconnection Traps	Shows if the SNMP agent sends a trap when a client disconnects from a captive portal.

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

```
(EdgeCore Switching) #show captive-portal trapflags

Client Authentication Failure Traps.............  Disable
Client Connection Traps.........................  Disable
Client Database Full Traps......................  Disable
Client Disconnection Traps......................  Disable
```

show captive-portal user

This command displays information about wireless users associated with a captive portal.

Format `show captive-portal user [`*`user-id`*` | group]`

Mode Privileged EXEC

Term	*Definition*
User ID	A numeric identifier for a wireless client associated with a captive portal.

Term	*Definition*
User Name	The name a wireless client associated with a captive portal.
Session Timeout	Shows the number of seconds to wait before terminating a session. A user is logged out once the session timeout is reached. If the value is set to 0 then the timeout is not enforced. The default value is 3600 (1 hour).
Idle Timeout	Shows the number of seconds a user can remain idle before being automatically logged out. If the value is set to 0 then the timeout is not enforced.The default value is 0.
Group ID	Numeric index for user group.
Group Name	If the verification mode is Local or RADIUS, assign an existing User Group to the captive portal or create a new group. All users who belong to the group are permitted to access the network through this portal. The User Group list is the same for all CP configurations on the switch.
Password Configured	Shows if a password is configured for this user.
Max Bandwidth Up (bytes/sec)	Shows the maximum speed, in bytes per second, that a client can transmit traffic when using the captive portal. This setting limits the bandwidth at which the client can send data into the network.
Max Bandwidth Down (bytes/sec)	Shows the maximum speed, in bytes per second, that a client can receive traffic when using the captive portal. This setting limits the bandwidth at which the client can receive data from the network.
Max Input Octets (bytes)	Shows the maximum number of bytes that a client is allowed to receive when using the captive portal. After this limit has been reached the user will be disconnected.
Max Output Octets (bytes)	Shows the maximum number of bytes that a client is allowed to transmit when using the captive portal. After this limit has been reached the user will be disconnected.
Max Total Octets (bytes)	Shows the maximum number of bytes the user is allowed to transfer (sum of bytes transmitted and received). After this limit has been reached the user will be disconnected.

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

```
(EdgeCore Switching) #show captive-portal user

                            Session  Idle
User ID       User Name       Timeout Timeout  Group ID      Group Name
------- -------------------- ------- -------- -------- ---------------------
1       steve                0       0        1        Default

(EdgeCore Switching) #show captive-portal user 1

User ID..................................... 1
User Name................................... steve
Password Configured......................... Yes
Session Timeout............................. 0
Idle Timeout................................ 0
Max Bandwidth Up (bytes/sec)................ 0
Max Bandwidth Down (bytes/sec).............. 0
Max Input Octets (bytes).................... 0
Max Output Octets (bytes)................... 0
Max Total Octets (bytes).................... 0
```

```
Group ID            Group Name
-------- --------------------------------
1        Default

(EdgeCore Switching) #show captive-portal user group

Group ID      Group Name       User ID       User Name
-------- -------------------- ------- ----------------------
1        Default              1       steve

(EdgeCore Switching) #show captive-portal user group 1

Group ID..................................... 1
Group Name................................... Default

User ID            User Name
------- --------------------------------
1       steve
```

statistics interval

Use this command to configure the interval at which peer switches report statistics on wireless clients associated with a captive portal. The valid range is 15-3600 seconds. Use 0 to disable reporting by peer switches.

Default 120

Format `statistics interval {0, 15-3600}`

Mode Captive Portal

no statistics interval

Use this command to reset the interval at which peer switches report statistics on wireless clients associated with a captive portal to the default setting or 120 seconds.

Format `no statistics interval`

Mode Captive Portal

timeout-msg

Use this command to enter the text used to display when the system has rejected authentication because the authentication transaction took too long. This could be due to user input time, or a timeout due to the overall transaction process.

Default Error: Timed Out, please reconnect and try again!

Format timeout-msg *<UTF-16>*

Mode Captive Portal Locale Configuration

no timeout-msg

Use this command to restore the default text used to display when the system has rejected authentication because the authentication transaction took too long.

Format no timeout-msg

Mode Captive Portal Locale Configuration

title-text

Use this command enter the text to use as the page title on the Authentication page.

Default Welcome to the Network!

Format title-text *<UTF-16>*

Mode Captive Portal Locale Configuration

no title-text

Use this command restore the default text to use as the page title on the Authentication page.

Format no title-text

Mode Captive Portal Locale Configuration

trapflags

Use this command to send SNMP traps from the captive portal or to specify certain captive portal events that will generate a trap.

Default Disabled

Format `trapflags [client-auth-failure | client-connect | client-db-full | client-disconnect]`

Mode Captive Portal

Parameter	*Definition*
client-auth-failure	The SNMP agent sends a trap when a client attempts to authenticate with a captive portal but is unsuccessful.
client-connect	The SNMP agent sends a trap when a client authenticates with and connects to a captive portal.
client-db-full	The SNMP agent sends a trap each time an entry cannot be added to the client database because it is full.
client-disconnect	The SNMP agent sends a trap when a client disconnects from a captive portal.

no trapflags

Use this command to stop SNMP traps from being sent from the captive portal or to stop certain captive portal events from generating a trap.

Format `no trapflags [client-auth-failure | client-connect | client-db-full | client-disconnect]`

Mode Captive Portal

user

Use this command to configure connection settings for a captive port user.

Format `user 1-8092 {account-generator | age-timeout | age-timeout-real | auto-gen-flag | idle-timeout | max-bandwidth-down | max-bandwidth-up | max-input-octets | max-output-octets | max-total-octets | session-timeout}`

Mode Captive Portal

Parameter	*Definition*
1-8092	A numeric identifier for a captive portal user.
age-timeout	The timeout for a user account. The range is 0-86400 seconds. The default is 0 which means no limit.
age-timeout-real	The remaining time before the user account is aged out. The range is 0-86400 seconds. The default is 0 which means no limit.
auto-gen-flag	Automatically generates a user name and password. The user name and password are a sequence of eight random alphanumeric characters.
idle-timeout	Sets the number of seconds a user can remain idle before being automatically logged out. If the value is set to 0 then the timeout is not enforced.The default value is 0.
max-bandwidth-down	Sets the maximum speed, in bytes per second, that a client can receive traffic when using the captive portal. This setting limits the bandwidth at which the client can receive data from the network. The range is 0-536870911 bytes per second. The default is 0 which means no limit.
max-bandwidth-up	Sets the maximum speed, in bytes per second, that a client can transmit traffic when using the captive portal. This setting limits the bandwidth at which the client can send data into the network.The range is 0-536870911 bytes per second. The default is 0 which means no limit.
max-input-octets	Sets the maximum number of bytes that a client is allowed to receive when using the captive portal. After this limit has been reached the user will be disconnected. The range is 0-4294967295 bytes. The default is 0 which means no limit.
max-output-octets	Sets the maximum number of bytes that a client is allowed to transmit when using the captive portal. After this limit has been reached the user will be disconnected. The range is 0-4294967295 bytes. The default is 0 which means no limit.
max-total-octets	Shows the maximum number of bytes the user is allowed to transfer (sum of bytes transmitted and received). After this limit has been reached the user will be disconnected. The range is 0-4294967295 bytes. The default is 0 which means no limit.
session-timeout	Sets the number of seconds to wait before terminating a session. A user is logged out once the session timeout is reached. If the value is set to 0 then the timeout is not enforced. The default value is 3600 (1 hour).

user group

Use this command to create a user group.

Format `user group 1-8092`

Mode Captive Portal

user group moveusers

Use this command to move all of the users in an existing group to a new group.

Format `user 1-8092 destination-group-id`

Mode Captive Portal

user group name

Use this command to assign a name to a user group. A name can contain 1 to 32 alphanumeric characters.

Format `user group 1-8092 name` *`name`*

Mode Captive Portal

user-label

Use this command to enter the text to display next to the field where the user enters the username.

Default Username

Format user-label *<UTF-16>*

Mode Captive Portal Locale Configuration

no user-label

Use this command to restore the default text to display next to the field where the user enters the username.

Format no user-label

Mode Captive Portal Locale Configuration

user name

Use this command to configure the name of a captive port user. A name can contain 1 to 32 alphanumeric characters.

Format `user name` *`name`*

Mode Captive Portal

user password

Use this command to configure the password of a captive port user. Enter this command without any parameters to enable password authentication for authentication via the local switch or RADIUS server. If a password is specified, it can contain 8 to 64 characters.

Format `user password [encrypted` *`encrypted-password`*`]`

Mode Captive Portal

welcome-text

Use this command to enter the text to display to further identify the network to be accessed by the CP user. This message displays under the Welcome Title.

Default You are now authorized and connected to the network.

Format welcome-text *<UTF-16>*

Mode Captive Portal Locale Configuration

no welcome-text

Use this command to restore the default text to display to further identify the network to be accessed by the CP user.

Format welcome-text *<UTF-16>*

Mode Captive Portal Locale Configuration

welcome-title

Use this command to enter the title to display to greet the user after he or she successfully connects to the network.

Default Congratulations!

Format welcome-title *<UTF-16>*

Mode Captive Portal Locale Configuration

no welcome-title

Use this command to restore the default title to display to greet the user after he or she successfully connects to the network.

Format no welcome-title

Mode Captive Portal Locale Configuration

wip-msg

Use this command to configure the message indicating that authentication is in progress. This message displays after the user clicks the button to connect to the network.

Default Connecting, please be patient.

Format wip-msg *<UTF-16>*

Mode Captive Portal Locale Configuration

no wip-msg

Use this command to restore the default message indicating that authentication is in progress.

Format no wip-msg

Mode Captive Portal Locale Configuration

radius-auth-server

Use this command to configure the name of the RADIUS authentication server used for client authentication. The switch acts as a RADIUS client and performs all RADIUS transactions on behalf of the clients. To configure RADIUS server information, go to Security > RADIUS > Server Configuration.

Default Default-RADIUS-Server

Format radius-auth-server *server-name*

Mode Captive Portal Configuration

no radius-auth-server

Use this command to restore the default name of the RADIUS authentication server used for client authentication.

Format radius-auth-server *server-name*

Mode Captive Portal Configuration

session-timeout

Use this command to configure the number of seconds the captive portal will wait before terminating a session. A user is logged out once the session timeout is reached. If the value is set to 0 then the timeout is not enforced.

Default 3600 (1 hour)

Format session-timeout *0-86400*

Mode Captive Portal Configuration

no session-timeout

Use this command to restore the default number of seconds the captive portal will wait before terminating a session.

Format session-timeout *0-86400*

Mode Captive Portal Configuration

user-logout

Use this command to allow an authenticated client to deauthenticate from the network. If this option is not selected or the user does not specifically request logout, the client connection status remains authenticated until the CP deauthenticates the user, for example by reaching the idle timeout or session timeout values.

Default Disabled

Format user-logout

Mode Captive Portal Configuration

no user-logout

Use this command to disallow an authenticated client from deauthenticating from the network.

Format user-logout

Mode Captive Portal Configuration

verification

Use this command to configure the mode which CP uses to verify clients – guest, local or RADIUS.

Default Guest

Format verification {guest | local | radius}

Mode Captive Portal Configuration

Term	*Definition*
guest	The user does not need to be authenticated by a database.
Local	The switch uses a local database to authenticate users.
radius	The switch uses a database on a remote RADIUS server to authenticate users.

RADIUS Commands

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

radius accounting mode

This command is used to enable the RADIUS accounting function.

Default disabled

Format `radius accounting mode`

Mode Global Config

no radius accounting mode

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

Format `no radius accounting mode`

Mode Global Config

radius server 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.

```
(EdgeCore Switching) (Config) #radius server attribute 4 192.168.37.60
(EdgeCore Switching) (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.

```
(EdgeCore Switching) (Config) #radius server host acct 192.168.37.60
(EdgeCore Switching) (Config) #radius server host acct 192.168.37.60 port 1813
(EdgeCore Switching) (Config) #radius server host auth 192.168.37.60 name Network1_RS port 1813
(EdgeCore Switching) (Config) #radius server host acct 192.168.37.60 name Network2_RS
(EdgeCore Switching) (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.

```
(EdgeCore Switching) #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.

```
(EdgeCore Switching) #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
```

```
(EdgeCore Switching) #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

(EdgeCore Switching) #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

(EdgeCore Switching) #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.

```
(EdgeCore Switching) #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


 (EdgeCore Switching) #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.
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.

```
(EdgeCore Switching) #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

(EdgeCore Switching) #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.

Term	*Definition*
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.

```
(EdgeCore Switching) #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

(EdgeCore Switching) #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
```

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 132) to capture the running configuration into a script. Use the `copy` command (see "copy" on page 143) 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

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

Section 3: Utility Commands

This chapter describes the utility commands available in the EWS4502/EWS4606 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.

```
(EdgeCore Switching) #show autoinstall

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

Dual Image Commands

EWS4502/EWS4606 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.

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] {A | B}`

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

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}`

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.

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

Term	*Definition*
Dot1x Statistics	• **EAPOL Frames 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*
Total Packets Received (Octets)	The total number of octets of data received by the processor (excluding framing bits but including FCS octets).
Packets Received Without Error	The total number of packets (including broadcast packets and multicast packets) received by the processor.
Unicast Packets Received	The number of subnetwork-unicast packets delivered to a higher-layer protocol.
Multicast Packets Received	The total number of packets received that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address.
Broadcast Packets Received	The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.
Receive Packets Discarded	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. A possible reason for discarding a packet could be to free up buffer space.
Octets Transmitted	The total number of octets transmitted out of the interface, including framing characters.
Packets Transmitted without Errors	The total number of packets transmitted out of the interface.
Unicast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
Multicast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to a Multicast address, including those that were discarded or not sent.
Broadcast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to the Broadcast address, including those that were discarded or not sent.
Transmit Packets Discarded	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. A possible reason for discarding a packet could be to free up buffer space.
Most Address Entries Ever Used	The highest number of Forwarding Database Address Table entries that have been learned by this switch since the most recent reboot.
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.

Term	*Definition*
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.

Format `show process cpu`

Mode Privileged EXEC

The following shows example CLI display output for the command.

```
(EdgeCore Switching) #show process cpu
Memory Utilization Report
Memory total : 1057894400
status      bytes
------ ----------
free    866889728
alloc   191004672

 CPU Utilization:

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

show process cpu threshold

This command displays CPU utilization and memory monitoring threshold information.

Format `show process cpu threshold`

Mode Privileged EXEC

The following shows example CLI display output for the command.

```
(EdgeCore Switching) #show process cpu threshold

CPU Utilization Monitoring Parameters
Rising Threshold.............................. 0 %
Rising Interval............................... 0 secs
Falling Threshold............................. 0 %
Falling Interval.............................. 0 secs

CPU Free Memory Monitoring Threshold.......... 0 KB
```

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.)

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 56.
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 56.
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 56.
System ObjectID	The base object ID for the switch's enterprise MIB.
System Up Time	The time in days, hours and minutes since the last switch reboot.
Current SNTP Synchronized Time	The system time synchronized from an SNTP server.
MIBs Supported	A list of MIBs supported by this agent.

show tech-support

Use the `show tech-support` command to display system and configuration information when you contact technical support. The output of the `show tech-support` command combines the output of the following commands:

- 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.

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 EWS4502/EWS4606 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 137 for a list of host indexes.

Format `logging host remove hostindex`

Mode Global Config

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

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.
Persistent Logging	Shows whether persistent logging is enabled.
Persistent Logging Severity Filter	The minimum severity to log for persistent logging. Messages with an equal or lower numerical severity are logged.
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.

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:

```
(EdgeCore Switching) # 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:

```
(EdgeCore Switching) # 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 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 captive-portal users

This command clears all captive portal data.

Format `clear captive-portal users`

Mode Privileged EXEC

clear traplog

This command clears the trap log.

Format `clear traplog`

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:

```
(EdgeCore Switching) #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:

```
(EdgeCore Switching) # 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:

```
(EdgeCore Switching) # 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.

Format `copy source destination`

Mode Privileged EXEC

Replace the *source* and *destination* parameters with the options in Table 9 on page 144. For the *url* source or destination, use:
`{xmodem | tftp://ipaddr|hostname | ip6address|hostname/filepath/filename [noval]}`

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.
`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:
`(EdgeCore Switching) #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 34.
`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 38.
`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.

Table 9: Copy Parameters (Cont.)

Source	*Destination*	*Description*
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.

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 client mode

This command enables Simple Network Time Protocol (SNTP) client mode and sets the mode to unicast.

Default disabled

Format `sntp client mode 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 10.

Default 6

Format `sntp unicast client poll-interval` *`poll-interval`*

Mode Global Config

no sntp unicast client poll-interval

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

Format `no sntp unicast client poll-interval`

Mode Global Config

sntp unicast client poll-timeout

This command 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 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 Unicast Attempt Time	Time of last transmit query (in unicast mode).
Last Attempt Status	Status of the last SNTP request (in unicast mode) or unsolicited message (in broadcast mode).

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

For each configured server:

Term	*Definition*
IP Address / Hostname	IP address or hostname of configured SNTP Server.
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.

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 EWS4502/EWS4606.

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 EWS4502/EWS4606 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

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.

```
<EdgeCore 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-detect

This command clears the detected address conflict status information.

Format `clear ip address-conflict-detect`

Modes Privileged EXEC
User EXEC

Serviceability Packet Tracing Commands

These commands improve the capability of network engineers to diagnose conditions affecting their EWS4502/ EWS4606 product.

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

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 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 packet [transmit | receive]`

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 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 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), S
RC_IP:10.50.50.1, DEST_IP:10.50.50.2, Type:ECHO_REPLY
```

The following parameters are displayed in the trace message:

Parameter	*Definition*
TX/RX	TX refers to a packet transmitted by the device. RX refers to packets received by the device.
Intf	The interface that the packet came in or went out on. Format used is unit/slot/port (internal interface number). Unit is always shown as 1 for interfaces on a non-stacking device.
SRC_IP	The source IP address in the IP header in the packet.
DEST_IP	The destination IP address in the IP header in the packet.
Type	Type determines whether or not the ICMP message is a REQUEST or a RESPONSE.

no debug ping packet

This command disables tracing of ICMP echo requests and responses.

Format `no debug ping 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

Section 4: Switching Commands

This chapter describes the switching commands available in the EWS4502/EWS4606 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 0/1:

```
(EdgeCore Switching) #configure
(EdgeCore Switching) (config)#interface 0/1
(EdgeCore Switching) (interface 0/1)#
```

Example: The following example enters Interface Config mode for ports 1/0/1 through 1/0/4:

```
(EdgeCore Switching) #configure
(EdgeCore Switching) (config)#interface 1/0/1-1/0/4
(EdgeCore Switching) (interface 1/0/1-1/0/4)#
```

description

Use this command to create an alpha-numeric description of an interface or range of interfaces.

Format `description description`

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

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 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 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 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 6 to 40.

Default 20

Format `spanning-tree max-hops {6—40}`

Mode Global Config

no spanning-tree max-hops

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

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

spanning-tree 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	Global 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 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

VLAN Commands

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

vlan database

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

Format `vlan database`

Mode Privileged EXEC

network mgmt_vlan

This command configures the Management VLAN ID.

Default 1

Format `network mgmt_vlan` *`1–4093`*

Mode Privileged EXEC

no network mgmt_vlan

This command sets the Management VLAN ID to the default.

Format `no network mgmt_vlan`

Mode Privileged EXEC

vlan

This command creates a new VLAN and assigns it an ID. The ID is a valid VLAN identification number (ID 1 is reserved for the default VLAN). VLAN range is 1–4093.

Format `vlan` *`1–4093`*

Mode VLAN Config

no vlan

This command deletes an existing VLAN. The ID is a valid VLAN identification number (ID 1 is reserved for the default VLAN). The VLAN range is 2–3965.

Format `no vlan` *`2–3965`*

Mode VLAN Config

vlan makestatic

This command changes a dynamically created VLAN (created by GVRP registration) to a static VLAN (one that is permanently configured and defined). The ID is a valid VLAN identification number. VLAN range is 2–4093.

Format `vlan makestatic` *`2–4093`*

Mode VLAN Config

vlan name

This command changes the name of a VLAN. The name is an alphanumeric string of up to 32 characters, and the ID is a valid VLAN identification number. ID range is 1–4093.

Default
- VLAN ID 1 - default
- other VLANS - blank string

Format `vlan name 1–4093 name`

Mode VLAN Config

no vlan name

This command sets the name of a VLAN to a blank string.

Format `no vlan name 1–4093`

Mode VLAN Config

vlan 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

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.

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.

clear radius statistics

This command is used to clear all RADIUS statistics.

Format `clear radius statistics`

Mode Privileged EXEC

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 max-req

This command sets the maximum number of times the authenticator state machine on 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.

Format `dot1x max-users` *count*

Mode Interface Config

no dot1x max-users

This command resets the maximum number of clients allowed per port to its default value.

Format `no dot1x max-users`

Mode Interface Config

dot1x port-control

This command sets the authentication mode to use on the specified interface or range of interfaces. Use the `force-unauthorized` parameter to specify that the authenticator PAE unconditionally sets the controlled port to unauthorized. Use the `force-authorized` parameter to specify that the authenticator PAE unconditionally sets the controlled port to authorized. Use the `auto` parameter to specify that the authenticator PAE sets the controlled port mode to reflect the outcome of the authentication exchanges between the supplicant, authenticator and the authentication server. If the `mac-based` option is specified, then MAC-based dot1x authentication is enabled on the port.

Default auto

Format `dot1x port-control {force-unauthorized | force-authorized | auto | mac-based}`

Mode Interface Config

no dot1x port-control

This command sets the 802.1X port control mode on the specified port to the default value.

Format `no dot1x port-control`

Mode Interface Config

dot1x 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 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. The guest-vlan-period must be a value in the range 1 - 300.
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 EWS4502/EWS4606). 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

802.1X Supplicant Commands

EWS4502/EWS4606 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` *user*

Mode Interface Config

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.

EWS4502/EWS4606 provides broadcast, multicast, and unicast story recovery for individual interfaces. Unicast Storm-Control protects against traffic whose MAC addresses are not known by the system. For broadcast, multicast, and unicast storm-control, if the rate of traffic ingressing on an interface increases beyond the configured threshold for that type, the traffic is dropped.

To configure storm-control, you will enable the feature for all interfaces or for individual interfaces, and you will set the threshold (storm-control level) beyond which the broadcast, multicast, or unicast traffic will be dropped. The Storm-Control feature allows you to limit the rate of specific types of packets through the switch on a per-port, per-type, basis.

Configuring a storm-control level also enables that form of storm-control. Disabling a storm-control level (using the `no` version of the command) sets the storm-control level back to the default value and disables that form of storm-control. Using the `no` version of the `storm-control` command (not stating a *`Level`*) disables that form of storm-control but maintains the configured *`Level`* (to be active the next time that form of storm-control is enabled.)

Note: The actual rate of ingress traffic required to activate storm-control is based on the size of incoming packets and the hard-coded average packet size of 512 bytes — used to calculate a packet-per-second (pps) rate - as the forwarding-plane requires pps versus an absolute rate kbps. For example, if the configured limit is 10%, this is converted to ~25000 pps, and this pps limit is set in forwarding plane (hardware). You get the approximate desired output when 512bytes packets are used.

storm-control broadcast

Use this command to enable broadcast storm recovery mode for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode). If the mode is enabled, broadcast storm recovery is active and, if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of broadcast traffic will be limited to the configured threshold.

Default	disabled
Format	`storm-control broadcast`
Mode	Global Config Interface Config

no storm-control broadcast

Use this command to disable broadcast storm recovery mode for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode).

Format	`no storm-control broadcast`

Mode Global Config
Interface Config

storm-control broadcast level

Use this command to configure the broadcast storm recovery threshold for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) as a percentage of link speed and enable broadcast storm recovery. If the mode is enabled, broadcast storm recovery is active, and if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic is dropped. Therefore, the rate of broadcast traffic is limited to the configured threshold.

Default 5

Format `storm-control broadcast level` *`0–100`*

Mode Global Config
Interface Config

no storm-control broadcast level

This command sets the broadcast storm recovery threshold to the default value for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) and disables broadcast storm recovery.

Format `no storm-control broadcast level`

Mode Global Config
Interface Config

storm-control broadcast rate

Use this command to configure the broadcast storm recovery threshold for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) in packets per second. If the mode is enabled, broadcast storm recovery is active, and if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic is dropped. Therefore, the rate of broadcast traffic is limited to the configured threshold.

Default 0

Format `storm-control broadcast rate` *`0–14880000`*

Mode Global Config
Interface Config

no storm-control broadcast rate

This command sets the broadcast storm recovery threshold to the default value for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) and disables broadcast storm recovery.

Format `no storm-control broadcast rate`

Mode Global Config
Interface Config

storm-control multicast

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

Default disabled

Format `storm-control multicast`

Mode Global Config
Interface Config

no storm-control multicast

This command disables multicast storm recovery mode for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode)

Format `no storm-control multicast`

Mode Global Config
Interface Config

storm-control multicast level

This command configures the multicast storm recovery threshold for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) as a percentage of link speed and enables multicast storm recovery mode. If the mode is enabled, multicast storm recovery is active, and if the rate of L2 multicast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of multicast traffic will be limited to the configured threshold.

Default 5

Format `storm-control multicast level` *`0–100`*

Mode Global Config
Interface Config

no storm-control multicast level

This command sets the multicast storm recovery threshold to the default value for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) and disables multicast storm recovery.

Format `no storm-control multicast level` *`0–100`*

Mode Global Config
Interface Config

storm-control multicast rate

Use this command to configure the multicast storm recovery threshold for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) in packets per second. If the mode is enabled, multicast storm recovery is active, and if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic is dropped. Therefore, the rate of multicast traffic is limited to the configured threshold.

Default 0

Format `storm-control multicast rate` *`0—14880000`*

Mode Global Config
Interface Config

no storm-control multicast rate

This command sets the multicast storm recovery threshold to the default value for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) and disables multicast storm recovery.

Format `no storm-control multicast rate`

Mode Global Config
Interface Config

storm-control unicast

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

Default disabled

Format `storm-control unicast`

Mode Global Config
Interface Config

no storm-control unicast

This command disables unicast storm recovery mode for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode).

Format `no storm-control unicast`

Mode Global Config
Interface Config

storm-control unicast level

This command configures the unicast storm recovery threshold for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) as a percentage of link speed, and enables unicast storm recovery. If the mode is enabled, unicast storm recovery is active, and if the rate of unknown L2 unicast (destination lookup failure) traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of unknown unicast traffic will be limited to the configured threshold.This command also enables unicast storm recovery mode for an interface.

Default 5

Format `storm-control unicast level` *`0—100`*

Mode Global Config
Interface Config

no storm-control unicast level

This command sets the unicast storm recovery threshold to the default value for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) and disables unicast storm recovery.

Format `no storm-control unicast level`

Mode Global Config
Interface Config

storm-control unicast rate

Use this command to configure the unicast storm recovery threshold for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) in packets per second. If the mode is enabled, unicast storm recovery is active, and if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic is dropped. Therefore, the rate of unicast traffic is limited to the configured threshold.

Default 0

Format `storm-control unicast rate` *`0—14880000`*

Mode Global Config
Interface Config

no storm-control unicast rate

This command sets the unicast storm recovery threshold to the default value for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) and disables unicast storm recovery.

Format `no storm-control unicast rate`

Mode Global Config
Interface Config

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

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 EWS4502/EWS4606 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 current session 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.
Admin 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.
Mirrored 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.

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:).

Denial of Service Commands

This section describes the commands you use to configure Denial of Service (DoS) Control. EWS4502/EWS4606 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.
- **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 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.
ICMPv4 Mode	May be enabled or disabled. The factory default is disabled.
Max ICMPv4 Payload Size	The range is 0–1023. The factory default is 512.
ICMPv6 Mode	May be enabled or disabled. The factory default is disabled.
Max ICMPv6 Payload Size	The range is 0–16384. The factory default is 512.
ICMP Fragment 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 FIN&URG& PSH Mode	May be enabled or disabled. The factory default is disabled.
TCP Flag & Sequence Mode	May be enabled or disabled. The factory default is disabled.
TCP SYN Mode	May be enabled or disabled. The factory default is disabled.
TCP SYN & FIN Mode	May be enabled or disabled. The factory default is disabled.
TCP Fragment Mode	May be enabled or disabled. The factory default is disabled.
TCP Offset Mode	May be enabled or disabled. The factory default is disabled.

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.

Default all

Format `show forwardingdb agetime`

Mode Privileged EXEC

Term	*Definition*
Address Aging Timeout	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.

Term	*Definition*
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*
Max MFDB Table Entries	The largest number of entries allowed in the Multicast Forwarding Database table.
Most MFDB Entries Since Last Reset	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.

Section 5: Routing Commands

This chapter describes the routing commands available in the EWS4502/EWS4606 CLI. The Routing Commands chapter contains the following sections:

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.

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 switch

This command displays the contents of the switch's Address Resolution Protocol (ARP) table.

Format `show arp switch`

Mode Privileged EXEC

Term	*Definition*
MAC Address	The hardware MAC address of that device.
IP Address	The IP address of a device on a subnet attached to the switch.
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.

renew dhcp network-port

Use this command to force the DHCPv4 client to immediately renew an IPv4 address lease.

Format `renew dhcp network-port`

Mode Privileged EXEC

Section 6: IPv6 Commands

This chapter describes the IPv6 commands available in the EWS4502/EWS4606 CLI.

IPv6 Management commands allow a device to be managed via an IPv6 address in a switch or IPv4 routing (i.e.,

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.

independent from the IPv6 Routing package). For Routing/IPv6 builds of the EWS4502 dual IPv4/IPv6 operation over the service port is enabled. The EWS4502 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.

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

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`* `[autoconfig | dhcp}`

Mode Privileged EXEC

Parameter	*Description*
address	IPv6 prefix in IPv6 global address format.

Parameter	*Description*
prefix-length	IPv6 prefix length value.
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

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 network link-local-address} [size datagram-size]}`

Mode Privileged EXEC
User Exec

traceroute ipv6

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

Format `traceroute ipv6 ipv6-address [port]`

Mode Privileged EXEC

Section 7: 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.

ac-load-balance-mode

This command enables AC load balance mode. When access controller (AC) switches are configured in a cluster, load balancing will ensure that each AC manages an even number of APs. In addition, the cluster supports redundancy between primary and secondary ACs. If the primary AC fails, the secondary AC will support the load until the primary AC recovers.

Format `ac-load-balance-mode`

Mode Global Config

no ac-load-balance-mode

This command disables AC load balance mode.

Format `no ac-load-balance-mode`

Mode Global Config

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.

```
(EdgeCore Switching) (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.

```
(EdgeCore Switching) (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

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

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 | 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.
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 | 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 | 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.
detected-client	Time in hours to maintain an entry in the detected clients database.
rf-scan	Time in hours to maintain an entry obtained from an RF scan.
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
- device-location—Enable
- discovery—Disable
- global—Enable
- known-client—Enable
- radius-client—Enable

Format `peer-switch configuration [{ap-database|ap-profile|captive-portal|channel-power|device-location|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.
device-location	Enable/Disable including AP and Client location information in the configuration that the switch pushes to its peers.
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|device-location|discovery|global|known-client|radius-client}]`

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.

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

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. Range is from 0 to 255.

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.

```
(EdgeCore Switching) #radius server-name auth  “Wireless_Auth-Server 1” ?
<cr>    Press Enter to execute the command.

(EdgeCore Switching) #no radius server-name auth ?
<cr>    Press Enter to execute the command.

(EdgeCore Switching) #radius server-name acct  “Wireless_Acct_Server 1” ?
<cr>    Press Enter to execute the command.

(EdgeCore Switching) #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.
Operational Status	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.
Wireless System IP control port	The TCP port used for AP control.
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.

Field	*Description*
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.

```
(EdgeCore Switching) #show wireless

Administrative Mode.......................... Enable
Operational Status........................... Enabled
WS IP Address................................ 192.168.1.1
WS Auto IP Assign Mode ...................... Enable
WS Switch Static IP ......................... 0.0.0.0
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
Cluster Priority............................. 1
Cluster Controller........................... Yes
Cluster Controller IP Address................ 192.168.1.1
Wireless System IP control port.............. 57775
AP Client QoS Mode........................... Disable
Switch Provisioning.......................... Enable
Network Mutual Authentication Mode........... Disable
Unmanaged AP Re-provisioning Mode............ Enable
Network Mutual Authentication Status.......... Not Started
Regenerate X.509 Certificate Status.......... Not In Progress
```

show wireless country-code

This **show wireless country-code** 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 license-management

This **show wireless license-management** command displays detailed information about each license uploaded to the Wireless Switch.

Format `show wireless license-management`

Mode Privileged EXEC

Field	*Description*
Total Certificate Valid Account	The maximum number of license certificates which can uploaded to the switch.
Total Local Certificate Valid Account	The number of valid license certificates uploaded to the switch.
Local Certificate File Index	The index to a local license certificate.
License Control ID	A unique identifier for this license certificate.
MAC Address	The AC's MAC address for this certificate.
Serial Number	The AC's serial number for this certificate.
Create Date	The date this certificate was created.
Vendor	The name of the license vendor.
Product Name	The AC product name for this certificate.
Reason	Specifies the authenticated result of license file after SSL verification: • OK: No error. • Invalid Certificate: There is no license file or file format is invalid. • Invalid MAC Length: The length of MAC address is invalid. • Invalid Serial Length: The length of serial number is invalid. • Invalid Product Length: The length of product name is invalid. • Invalid MAC: The format of MAC address is invalid. • Invalid Serial: The format of serial number is invalid. • Invalid Licence-ID Repeat: The file owns duplicated License Control ID.
Authentication Account	Identifies the number of manageable AP for license file.

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

```
(EdgeCore Switching) #show wireless license-management

Total Certificate Valid Account.............. 31
Total Local Certificate Valid Account.......... 25

----------------------------------------------------------------
Local Certificate File Index: 1
License Control ID........................... 2014310001
MAC Address.................................. 7072CFCF9B4E
Serial Number................................ EC1436000105
Create Date.................................. 20141105
Vendor....................................... EDGECORE
Product Name................................. EWS4502
Reason....................................... OK
Authentication Account....................... 25
.
.
.
Local Certificate File Index: 10
License Control ID...........................
MAC Address..................................
Serial Number................................
Create Date..................................
Vendor.......................................
```

```
Product Name.................................
Reason..................................... Invalid Certificate
Authentication Account..................... 0
```

show wireless license-request

This **show wireless license-request** command displays the information which must be provided to a license supplier when requesting an AP operating license.

Format `show wireless license-request`

Mode Privileged EXEC

Field	*Description*
Base MAC Address	The MAC address of the AP which will use this license.
Serial Number	The serial number of the AP which will use this license.
Product Name	The product name of the AP which will use this license.

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

```
(EdgeCore Switching) #show wireless license-request


Please send below information to your License Supplier for license request.

Base MAC Address.............................. 70:72:CF:CF:9B:4E
Serial Number................................. EC1436000105
Product Name.................................. EWS4502
```

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.

```
(EdgeCore Switching) #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*
Number of Configurable Entries	Shows the maximum number of IP addresses that can be configured in the IP Discovery list.
Total Number of Configured Entries	Shows the number of IP addresses that have been configured in the IP Discovery list.
Total Number of Polled Entries	Identifies how many of the IP addresses in the IP Discovery list the switch has attempted to contact.
Total Number of Not-Polled Entries	Identifies how many of the IP addresses in the IP Discovery list the switch has not attempted to contact.
Total Number of Discovered Entries	Identifies how many devices (peer switches or APs) the switch has successfully discovered, authenticated, and validated by polling the IP address configured in the IP Discovery list.
Total Number of Discovered-Failed Entries	Identifies how many devices that have an IP address configured in the IP Discovery list that the switch has attempted to contact and failed to authenticate or validate.
IP Address	Shows the IP address of the device configured in the 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.

```
(EdgeCore Switching) #show wireless discovery ip-list

Maximum Number of Configurable Entries..... 256
Total Number of Configured Entries..... 2
Total Number of Polled Entries..... 0
Total Number of Not-Polled Entries..... 2
Total Number of Discovered Entries..... 0
Total Number of Discovered-Failed Entries..... 0
IP Address        Status
---------------   ------------------
10.27.21.12       Not Polled
10.27.225.157     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.

```
(EdgeCore Switching) #show wireless discovery vlan-list

VLAN List
-------------------------------------
1 - default
100 - techpubs
```

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.

Field	*Description*
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.
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.
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.
Maximum APs in WDS Group	The maximum number of APs allowed in a Wireless Distribution System (WDS) group.

Field	*Description*
Maximum WDS Links in WDS Group	The maximum number of WDS Links allowed in a Wireless Distribution System (WDS) group.

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

```
(EdgeCore Switching) #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...................  45000
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
Maximum APs in WDS Group.....................  64
Maximum WDS Links in WDS Group...............  0
```

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.

Field	*Description*
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.

```
(EdgeCore Switching) #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.
AC Load Balance	When access controller (AC) switches are configured in a cluster, load balancing is used to ensure that each AC manages an even number of APs.
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.

Field	*Description*
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:

```
(EdgeCore Switching) show wireless switch 10.27.65.8 status

Switch IP Address.............................. 10.27.65.8
AC Load Balance................................ Disable
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:

```
(EdgeCore Switching) #show wireless switch 192.168.37.60 status
Error! Only Cluster Controller can display the peer switch status parameters.

(EdgeCore Switching) #show wireless switch 192.168.37.61 status
Switch IP Address.............................. 192.168.37.61
AC Load Balance................................ Disable
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:

```
(EdgeCore Switching) #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

(EdgeCore Switching) #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:

```
(EdgeCore Switching) #show wireless switch 192.168.37.60 statistics <cr>
Error! Only Cluster Controller can display the peer switch statistics.
(EdgeCore Switching) #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:

```
(EdgeCore Switching) #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 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.

```
(EdgeCore Switching) #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 EWS4502/EWS4606 **show trapflags** command is modified to show the global Wireless Switch trap configuration. See the command "show trapflags" on page 63.

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.

```
(EdgeCore Switching) #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.
QoS DiffServ	Displays whether QoS DiffServ (classes, services, and policies) configuration push to peer switches is enabled or disabled.
WDS Group	Displays whether WDS group configuration information is pushed to peers.
Device Location	Displays whether Device Location configuration information is pushed to peers.

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

```
(EdgeCore Switching) #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
WDS Group....................................... Enable
Device Location................................. 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*
Configuration Request Status	The global status for the configuration push request.

Field	*Description*
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.
Peer IP Address	The peer switch IP Address.
Configuration Request Status	Configuration push status for the peer switch.

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

```
(EdgeCore Switching) #show wireless configuration request status

Configuration Request 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*
Configuration Receive Status	Indicates the status of the configuration push receive from the peer switch.
Peer Switch IP Address	The peer switch IP address that pushed configuration.
Configuration	Indicates the configuration groups received as part of the configuration push.
Timestamp	Indicates the configuration push received time.

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

```
(EdgeCore Switching) #show wireless configuration receive status

Configuration Receive Status.................. Not Started
```

```
Last Configuration Received
---------------------------
Peer Switch IP Address..... 0.0.0.0
Configuration.............. None
Timestamp.................. Jan  1 00:00:00 1970
```

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 | dual-boot | image-table]`

Mode Privileged EXEC

Field	*Description*
hw-id	The AP hardware type ID. The range is 1–20
radio-id	The radio index on the AP hardware type. The range is 1–2
dual-boot	Displays the AP Dual Boot Support table.
image-table	Displays the AP image capability table.
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.
VAP Count Per Radio	Number of virtual access points supported by this radio.
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.
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.

```
(EdgeCore Switching) #show wireless ap capability

Hardware  Hardware                                Radio  VAP Count  Image
Type ID   Type Description                       Count  Per Radio  Type
--------  --------------------------------------  -----  ---------  --------
1         MJ Dual Radio a/b/g                     2      4          2
2         MJ Single Radio a/b/g                   1      4          2
3         MJ Dual Radio a/b/g/n                   2      4          2
4         MJ Single Radio a/b/g/n                 1      4          2
5         Enterprise Dual Radio a/b/g/n           2      16         1
6         Enterprise Single Radio a/b/g/n         1      16         1
7         AP-64 Single Radio a/b/g/n              1      4          3
8         AP-66 Dual Radio a/b/g/n                2      16         3
```

```
9          Enterprise 4748 Dual Radio a/b/g/n        2      16         4
10         EAP7151A Single Radio b/g/n               1      16         5
11         EAP7011CA Single Radio b/g/n              1      16         5
12         EAP9012CA Dual Radio a/b/g/n              2      16         5
13         OAP9112CA Dual Radio a/b/g/n              2      16         5
14         EAP9112A Dual Radio a/b/g/n               2      16         5
15         EAP7015A Single Radio b/g/n               1      16         5
16         EAP7315A Single Radio b/g/n               1      16         5
17         EAP7311A Single Radio b/g/n               1      16         5
18         EAP9012A Dual Radio a/b/g/n               2      16         5
```

```
(EdgeCore Switching) #show wireless ap capability 6 radio 1

Hardware Type ID..................... 6
Hardware Type Description............ MJ Single Radio Accton a/b/g/n
Radio Count.........................1
Image Type.......................... 1-MJ Development Board

Radio...............................1
Radio Type Description.............Broadcom Enterprise a/b/g/n
VAP Count...........................8
802.11a Support.....................Enable
802.11bg Support....................Enable
802.11n Support.....................Enable
```

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.

```
(EdgeCore Switching) #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.

```
(EdgeCore Switching) # 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.

```
(EdgeCore Switching) #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.

Field	*Description*
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.

```
(EdgeCore Switching) #show wireless radius
RADIUS Authentication Server Name.......... Default-RADIUS-Server
RADIUS Authentication Server Status........ Configured
RADIUS Accounting Server Name.............. Default-RADIUS-Server
RADIUS Accounting Server Status............ Not Configured
RADIUS Accounting.......................... Disable
```

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.

```
(EdgeCore Switching) # show wireless mac-authentication-mode
MAC Authentication Mode..................... white-list
```

show wireless known-client

This show command displays the content of the local Known Client database.

Format	`show wireless known-client`
Mode	Privileged EXEC

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

(EdgeCore Switching) #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.

```
(EdgeCore Switching) #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.

(EdgeCore Switching) #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

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.

```
(EdgeCore Switching) (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 15

Format `power plan interval {15-1440}`

Mode Wireless Config

Parameter	*Description*
15–1440	The power plan interval in minutes.

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} {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.
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 {apply | clear | start}`

Mode Privileged EXEC

Parameter	*Description*
apply	Apply the proposed power adjustments.
clear	Clear the proposed power adjustments.
start	Compute new proposed power adjustments.

Example: This command can be executed after the power-plan algorithm is started and the proposed power value appears. Otherwise, the following error message will appear.

```
(EdgeCore Switching) #wireless power-plan apply

Unable to apply manual proposed power adjustment. The power adjustment status
is not in the proper state for the apply operation.
```

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. This 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}`

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.
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.
Last Iteration	Indicates the last iteration of the channel plan.
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.

```
(EdgeCore Switching) #show wireless channel-plan history a

Operational Status............................ Active
Last Iteration................................ 1
Last Algorithm Time........................... Jan  1 07:38:54 1970

AP MAC Address    Location                          Radio Iteration  Channel
----------------- --------------------------------- ----- ---------- -------
70:72:CF:89:01:40                                   2     1          36
```

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. This command displays a proposed summary for all peer switches.

Format `show wireless channel-plan proposed {an | bgn}`

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 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.
Old Channel	The previous channel used 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.

```
(EdgeCore Switching) #show wireless channel-plan proposed a

Current Status.............................. Algorithm Completed

                                                        Old     New
AP MAC Address    Location                          Radio Channel Channel
----------------- --------------------------------- ----- ------- -------
70:72:CF:89:01:40                                   2     157     36
```

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. This command displays a proposed summary for all peer switches.

Format `show wireless power-plan proposed`

Mode Privileged EXEC

Field	*Description*
ipaddr	A valid IP address.
Current Status	Indicates the status of a manual power adjustment request.

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

```
(EdgeCore Switching) #show wireless power-plan proposed
Switch IP Address  Current Status
-----------------  ---------------
10.254.22.1        Algorithm Completed
10.254.22.15       Algorithm Completed

(EdgeCore Switching) #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.
Cluster Controller IP Address	The IP address of the cluster controller.
Peer Switches	The number of peer switches managed by the cluster controller
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.
Age	Time since last update was received from the switch.
Managed AP Count	Total number of access points currently managed by the peer switch.
L2 Tunnel Interface	The designation for a layer 2 tunnel interface – a logical point-to-point link that carries encapsulated packets.

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

```
(EdgeCore Switching) #show wireless peer-switch

Cluster Controller IP Address.................. 192.168.0.22
Peer Switches.............................. 1

                 Vendor    Software             Protocol  Disc.
IP Address       ID        Version              Version   Reason      Age
---------------  ------   --------------------  --------  ---------  -----------
192.168.0.33     Edge-Core 1.0.10.7             2         L2 Poll 0d:00:00:14

(EdgeCore Switching) #show wireless peer-switch 10.254.22.1

IP Address..................................... 192.168.0.33
Vendor ID...................................... Edge-Core
Software Version............................... 1.0.10.7
Protocol Version............................... 2
```

```
Discovery Reason.............................. L2 Poll
Managed AP Count.............................. 0
L2 Tunnel Interface........................... 7/1
Age........................................... 0d:00:00:15
```

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.
Timestamp	The time the config push was received from the peer switch.

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

```
(EdgeCore Switching) #show wireless peer-switch configure status

                  Configuration
Peer IP Address  Switch IP Address  Configuration Status      Timestamp
---------------  -----------------  --------------------  --------------------
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

(EdgeCore Switching) #show wireless peer-switch 10.0.0.100 configure status

Peer Switch 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
Timestamp.................                    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.

```
(EdgeCore Switching) #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      14
00:01:01:02:02:01 192.168.0.100     Ground Floor   1-Default      14
00:01:01:02:03:0  192.168.0.200     Conf Room…     2-L3 Roaming.. 14
00:01:01:02:04:01 192.168.0.300     First Floor    3-WPA2 VAPs..  14

(EdgeCore Switching) #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      14
00:01:01:02:02:01 192.168.0.100 Ground Floor   1-Default      14


(EdgeCore Switching) #show wireless peer-switch ap 00:01:01:02:02:01 status

MAC address..................................... B8:9B:C9:FD:B0:80
Peer Switch IP Address.......................... 192.168.0.33
IP Address...................................... 192.168.0.5
IP Subnet Mask.................................. 255.255.255.0
Location........................................ Conf Room Bldg 200
Profile......................................... 2-ECW5110-L
Hardware Type................................... 14
```

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.

```
(EdgeCore Switching) (Config-ap)# password ?
<cr>Press Enter to execute the command.

(EdgeCore Switching) (Config-ap)# password <cr>
Enter Password (8 - 63 characters):<enter here>
Re-enter password:<enter same here>

(EdgeCore Switching) (Config-ap)# no password <cr>
(EdgeCore Switching) (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 {1-500}`

Mode AP Config

Parameter	*Description*
1–500	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.
Standalone Expected Channel	Expected channel for stand-alone mode.

Field	*Description*
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.

```
(EdgeCore Switching) #show wireless ap database 11:33:44:55:66:77

AP MAC Address.............................. 11:33:44:55:66:77
Location.................................... factory
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

(EdgeCore Switching) #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

security mode

This command configures the authentication and encryption mode on the network.

Default none
Format `security mode {none | static-wep | 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.
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 *EWS4502/EWS4606 Administrator's Guide*.

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.

```
(EdgeCore Switching) #radius server-name auth  “Wireless_Network-1 Auth_Server 1” ?
<cr>    Press Enter to execute the command.

(EdgeCore Switching) #no radius server-name auth ?
<cr>    Press Enter to execute the command.

(EdgeCore Switching) #radius server-name acct  “Wireless_Network-1 Acct_Server 1” ?
<cr>    Press Enter to execute the command.

(EdgeCore Switching) #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.

```
(EdgeCore Switching) # radius use-network-configuration ?
<cr>Press Enter to execute the command.

(EdgeCore Switching) # 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

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-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 {1-1440}`

Mode Network Config

Parameter	*Description*
1–1440	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, 30-86400}`

Mode Network Config

Parameter	*Description*
0, 30–86400	The session-key-refresh-rate range is 0 or 30 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

dist-tunnel

This command enables distributed L2 tunneling on the wireless controller switch. The distributed L2 tunneling mode supports L3 roaming for wireless clients without forwarding any data traffic to the UWS. Use this command to enable or disable the mode.

Default Disabled
Format `dist-tunnel`
Mode Network Config

no dist-tunnel

The `no` version of this command disables distributed L2 tunneling on the wireless controller switch.

Format `no dist-tunnel`
Mode Network Config

vap-client-qos

This command enables the mapping of client traffic to a specified QoS priority value for the wireless network.

Default Disabled
Format `vap-client-qos`
Mode Network Config

no vap-client-qos

The `no` version of this command disables the mapping of client traffic to a specified QoS priority value.

Format `no vap-client-qos`
Mode Network Config

vap-client-qos-priority

This command specifies the default 802.1p QoS value for client traffic on the wireless network.

Default 0
Format `vap-client-qos-priority {0-7}`
Mode Network Config

Parameter	*Description*
0-7	The 802.1p QoS values are from 0 (low priority) to 7 (high priority).

no vap-client-qos-priority

The no version of this command restores the QoS priority to its default value.

Format `no vap-client-qos-priority`

Mode Network Config

vap-dhcp-relay

This command enables DHCP relay for the wireless network.

Dynamic Host Configuration Protocol (DHCP) can dynamically allocate an IP address and other configuration information to network clients that broadcast a request. To receive the broadcast request, the DHCP server would normally have to be on the same subnet as the client. However, when the DHCP relay agent is enabled, received client requests can be forwarded directly to a known DHCP server on another subnet. Responses from the DHCP server are returned to the switch, which then broadcasts them back to clients.

Default Disabled

Format `vap-dhcp-relay`

Mode Network Config

no vap-dhcp-relay

The no version of this command disables DHCP relay for the wireless network.

Format `no vap-dhcp-relay`

Mode Network Config

vap-dhcp-relay-ip

This command configures the DHCP relay server IP address for the wireless network.

Default 0.0.0.0

Format `vap-dhcp-relay-ip {ipaddr}`

Mode Network Config

Parameter	*Description*
ipaddr	The IP address of the DHCP relay server.

no vap-dhcp-relay

The no version of this command restores the default setting for the DHCP relay server IP address.

Format `no vap-dhcp-relay-ip`

Mode Network Config

vap-max-clients

This command configures the maximum number of clients for the wireless network.

Default 100

Format `vap-max-clients {1-100}`

Mode Network Config

Parameter	*Description*
1-100	The maximum number of wireless clients.

no vap-max-clients

The no version of this command restores the default setting for the maximum number of wireless clients.

Format `no vap-max-clients`

Mode Network Config

max-sta-dl-rate

This command configures the maximum down-link traffic rate for clients in the wireless network.

Default 65535 Kbps

Format `max-sta-dl-rate {10-65535}`

Mode Network Config

Parameter	*Description*
10-65535	The maximum traffic rate in Kbps.

no max-sta-dl-rate

The no version of this command restores the default setting for the maximum down-link rate for clients.

Format `no max-sta-dl-rate`

Mode Network Config

max-sta-up-rate

This command configures the maximum up-link traffic rate for clients in the wireless network.

Default 65535 Kbps
Format `max-sta-up-rate {10-65535}`
Mode Network Config

Parameter	*Description*
10-65535	The maximum traffic rate in Kbps.

no max-sta-up-rate

The `no` version of this command restores the default setting for the maximum up-link rate for clients.

Format `no max-sta-up-rate`
Mode Network Config

max-vap-dl-rate

This command configures the maximum down-link traffic rate for all clients in the VAP wireless network.

Default 65535 Kbps
Format `max-vap-dl-rate {10-65535}`
Mode Network Config

Parameter	*Description*
10-65535	The maximum traffic rate in Kbps.

no max-vap-dl-rate

The `no` version of this command restores the default setting for the maximum down-link rate for a VAP.

Format `no max-vap-dl-rate`
Mode Network Config

max-vap-up-rate

This command configures the maximum up-link traffic rate for all clients in the VAP wireless network.

Default 65535 Kbps
Format `max-vap-up-rate {10-65535}`
Mode Network Config

Parameter	*Description*
10-65535	The maximum traffic rate in Kbps.

no max-vap-up-rate

The `no` version of this command restores the default setting for the maximum up-link rate for all VAP clients.

Format `no max-vap-up-rate`
Mode Network Config

acl-mac-mode

This command enables ACL filtering of MAC addresses denied access to the network.

Default Disabled
Format `acl-mac-mode`
Mode Network Config

no acl-mac-mode

The `no` version of this command disables MAC ACL filtering.

Format `no acl-mac-mode`
Mode Network Config

acl-mac-list

This command configures a list of MAC addresses denied access to the network.

Default None configured
Format `acl-mac-list {macaddr}`
Mode Network Config

Parameter	*Description*
macaddr	A wireless client MAC address.

no acl-mac-list

The no version of this command removes all MAC addresses from the list.

Format `no acl-mac-list`

Mode Network Config

vap-tun-switch-type

This command configures a data tunnel for the VAP wireless network.

Default Disabled

Format `vap-tun-switch-type {capwap | disable}`

Mode Network Config

Parameter	*Description*
disable	Disables the data protocol tunnel.
CAPWAP	Enables a CAPWAP protocol tunnel

no vap-tun-switch-type

The no version of this command restores the default setting for the data tunnel.

Format `no vap-tun-switch-type`

Mode Network Config

vap-tun-switch-ip

This command configures the primary switch IP address for an Individual CAPWAP data tunnel.

Default 0.0.0.0

Format `vap-tun-switch-ip {ipaddr}`

Mode Network Config

Parameter	*Description*
ipaddr	The primary controller switch IP address when the Individual CAPWAP tunnel type is selected.

no vap-tun-switch-ip

The no version of this command restores the default setting for the primary controller switch IP address.

Format `no vap-tun-switch-ip`

Mode Network Config

vap-tun-switch-port

This command configures the primary switch UDP port number for an Individual CAPWAP data tunnel.

Default 30000

Format `vap-tun-switch-port {1024-65535}`

Mode Network Config

Parameter	*Description*
1024-65535	The primary controller switch UDP port number when the Individual CAPWAP tunnel type is selected.

no vap-tun-switch-port

The no version of this command restores the default setting for the primary controller switch UDP port number.

Format `no vap-tun-switch-port`

Mode Network Config

vap-tun-switch-2th-ip

This command configures the secondary switch IP address for an Individual CAPWAP data tunnel.

Default 0.0.0.0

Format `vap-tun-switch-2th-ip {ipaddr}`

Mode Network Config

Parameter	*Description*
ipaddr	The secondary controller switch IP address when the Individual CAPWAP tunnel type is selected.

no vap-tun-switch-2th-ip

The no version of this command restores the default setting for the secondary controller switch IP address.

Format `no vap-tun-switch-2th-ip`

Mode Network Config

vap-tun-switch-2th-port

This command configures the secondary switch UDP port number for an Individual CAPWAP data tunnel.

Default 30000
Format `vap-tun-switch-2th-port {1024-65535}`
Mode Network Config

Parameter	*Description*
1024-65535	The secondary controller switch UDP port number when the Individual CAPWAP tunnel type is selected.

no vap-tun-switch-2th-port

The `no` version of this command restores the default setting for the secondary controller switch UDP port number.

Format `no vap-tun-switch-2th-port`
Mode Network Config

gre-br-client-gw-ip

This command configures the GRE tunnel bridge mode gateway IP address for client APs.

Default 0.0.0.0
Format `gre-br-client-gw-ip {ipaddr}`
Mode Network Config

Parameter	*Description*
ipaddr	The gateway IP address for the GRE tunnel in bridge mode.

no gre-br-client-gw-ip

The `no` version of this command restores the default setting for the GRE tunnel bridge mode gateway IP address.

Format `no gre-br-client-gw-ip`
Mode Network Config

gre-br-client-netmask

This command configures the GRE tunnel bridge mode gateway netmask for client APs. The gateway netmask and tunnel bridge netmask are always identical.

Default 255.255.0.0

Format `gre-br-client-netmask {netmask}`

Mode Network Config

Parameter	*Description*
netmask	The gateway netmask for the GRE tunnel in bridge mode.

no gre-br-client-netmask

The `no` version of this command restores the default setting for the GRE tunnel bridge mode gateway netmask.

Format `no gre-br-client-netmask`

Mode Network Config

gre-br-ip

This command configures the IP address of the GRE tunnel interface on the controller.

Default 0.0.0.0

Format `gre-br-ip {ipaddr}`

Mode Network Config

Parameter	*Description*
ipaddr	The IP address for the GRE tunnel interface on the controller.

no gre-br-ip

The `no` version of this command restores the default setting for the GRE tunnel interface IP address.

Format `no gre-br-ip {ipaddr}`

Mode Network Config

gre-br-printer1-ip

This command configures a primary local printer IP address. Allows a local printer IP address to be mapped within an AP so printer changes do not affect settings on user devices.

Default 0.0.0.0
Format `gre-br-printer1-ip {ipaddr}`
Mode Network Config

Parameter	*Description*
ipaddr	The IP address of the local printer.

no gre-br-printer1-ip

The `no` version of this command restores the default setting for the primary local printer IP address.

Format `no gre-br-printer1-ip`
Mode Network Config

gre-br-printer2-ip

This command configures a secondary local printer IP address. Allows a local printer IP address to be mapped within an AP so printer changes do not affect settings on user devices.

Default 0.0.0.0
Format `gre-br-printer2-ip {ipaddr}`
Mode Network Config

Parameter	*Description*
ipaddr	The IP address of the local printer.

no gre-br-printer2-ip

The `no` version of this command restores the default setting for the secondary local printer IP address.

Format `no gre-br-printer2-ip`
Mode Network Config

gre-local-client-mss

This command configures the local maximum segment size (MSS) for TCP connection over the GRE tunnel. The maximum segment size is the largest amount of data, specified in octets, that can be received in a single TCP segment.

Default 0

Format `gre-local-client-mss {0, 512-1400}`

Mode Network Config

Parameter	*Description*
0, 512-1400	The TCP maximum segment size in bytes. When set to 0, the MSS is dynamically negotiated on the link.

no gre-local-client-mss

The `no` version of this command restores the default setting for the local MSS.

Format `no gre-local-client-mss`

Mode Network Config

gre-remote-client-mss

This command configures the remote maximum segment size (MSS) for TCP connection over the GRE tunnel. The maximum segment size is the largest amount of data, specified in octets, that can be received in a single TCP segment.

Default 0

Format `gre-remote-client-mss {0, 512-1400}`

Mode Network Config

Parameter	*Description*
0, 512-1400	The TCP maximum segment size in bytes. When set to 0, the MSS is dynamically negotiated on the link.

no gre-remote-client-mss

The `no` version of this command restores the default setting for the local MSS.

Format `no gre-remote-client-mss`

Mode Network Config

gre-tun-intf-ip

This command configures the GRE tunnel interface IP address.

Default 0.0.0.0
Format `gre-tun-intf-ip {ipaddr}`
Mode Network Config

Parameter	*Description*
ipaddr	The IP address of the GRE tunnel interface.

no gre-tun-intf-ip

The `no` version of this command restores the default setting for the GRE tunnel interface.

Format `no gre-tun-intf-ip`
Mode Network Config

gre-tun-intf-netmask

This command configures the GRE tunnel interface netmask.

Default 0.0.0.0
Format `gre-tun-intf-netmask {netmask}`
Mode Network Config

Parameter	*Description*
netmask	The IP netmask of the GRE tunnel interface.

no gre-tun-intf-netmask

The `no` version of this command restores the default setting for the GRE tunnel interface.

Format `no gre-tun-intf-netmask`
Mode Network Config

gre-tun-local-ip

This command configures the GRE tunnel local IP address.

Default 0.0.0.0
Format `gre-tun-local-ip {ipaddr}`
Mode Network Config

Parameter	*Description*
ipaddr	The IP address of the local end of the GRE tunnel.

no gre-tun-local-ip

The `no` version of this command restores the default setting for the GRE tunnel interface.

Format `no gre-tun-local-ip`
Mode Network Config

gre-tun-remote-intf-ip

This command configures the GRE tunnel remote interface IP address.

Default 0.0.0.0
Format `gre-tun-remote-intf-ip {ipaddr}`
Mode Network Config

Parameter	*Description*
ipaddr	The IP address of the GRE tunnel remote interface.

no gre-tun-remote-intf-ip

The `no` version of this command restores the default setting for the GRE tunnel interface.

Format `no gre-tun-remote-intf-ip`
Mode Network Config

gre-tun-remote-ip

This command configures the GRE tunnel remote IP address.

Default 0.0.0.0
Format `gre-tun-remote-ip {ipaddr}`
Mode Network Config

Parameter	*Description*
ipaddr	The IP address of the remote end of the GRE tunnel.

no gre-tun-remote-ip

The `no` version of this command restores the default setting for the GRE tunnel.

Format `no gre-tun-remote-ip`
Mode Network Config

gre-vap-tun-mode

This command selects Bridge or Router modes for a GRE tunnel.

Default 0 seconds
Format `gre-vap-tun-mode {bridge | router}`
Mode Network Config

Parameter	*Description*
bridge	The keyword that selects Bridge mode for a GRE tunnel.
router	The keyword that selects Router mode for a GRE tunnel.

gre-vap-intf-ip

This command configures the GRE tunnel interface IP address for a specific VAP.

Default 0.0.0.0
Format `gre-vap-intf-ip {ipaddr}`
Mode Network Config

Parameter	*Description*
ipaddr	The IP address of the VAP GRE tunnel interface.

no gre-vap-intf-ip

The no version of this command restores the default setting for the VAP GRE tunnel interface.

Format no gre-vap-intf-ip

Mode Network Config

gre-vap-intf-netmask

This command configures the GRE tunnel interface IP netmask for a specific VAP.

Default 255.255.255.0

Format gre-vap-intf-netmask {netmask}

Mode Network Config

Parameter	*Description*
netmask	The IP netmask of the VAP GRE tunnel interface.

no gre-vap-intf-netmask

The no version of this command restores the default setting for the VAP GRE tunnel interface.

Format no gre-vap-intf-netmask

Mode Network Config

gre-vap-vlan-id

This command configures the VLAN that serves as the bridge mode GRE tunnel interface on the controller.

Default 1

Format gre-vap-vlan-id {1-4094}

Mode Network Config

Parameter	*Description*
1-4094	The VLAN ID for the GRE tunnel interface.

no gre-vap-vlan-id

The no version of this command restores the default setting for the GRE tunnel VLAN.

Format no gre-vap-vlan-id

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*
Network ID	The ID associated with the network.
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
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 Status	Indicates whether the specified named RADIUS Authentication server is configured in the RADIUS Client configuration.
RADIUS Accounting Server Name	RADIUS server name for accounting.
RADIUS Accounting Server Status	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.

Field	*Description*
WPA Key Type	Specifies the type of the WPA key configured (ASCII only).
WPA Key	The WPA passphrase.
WPA2 Pre-Authentication	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.
Client Preemption Mode	Client preemption assigns a higher connection priority for clients using 802.11n when maximum capacity is reached.
Bandwidth Equal Share	If you enable this feature and VAP Bandwidth limitation, the AP will divide the total bandwidth equally among its clients.

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

```
(EdgeCore Switching) #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

(EdgeCore Switching) #show wireless network 3

Network ID..................................... 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
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
WPA Key.....................................
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................ -----
Client QoS Diffserv Policy Up.................. -----
Client Preemption Mode......................... Disable
Bandwidth Equal Share.......................... Disable
```

IP-ACL Commands

The IP-ACL by VAP feature is a software implementation that allows users (UDP/TCP ports) access to Internet or not. If an IP-ACL rule is defined, IP source to destination traffic can access Internet through the AP depending on the rule match and action taken (deny or permit). Every VAP can select a specific policy or not use any policy.

The following example shows how to configure an IP ACL and assign it to a VAP.

```
(EdgeCore Switching) #wireless
(EdgeCore Switching) (Config-wireless)#network 21
(EdgeCore Switching) (Config-network)#ip-acl-policy RD
(EdgeCore Switching) (Config-network)#exit
(EdgeCore Switching) (Config-wireless)#acl-ip-list 1.1.1.1 255.255.255.0 2.2.2.2 0.0.0.0 20 21 1 3 RD
(EdgeCore Switching) (Config-wireless)#network 21
(EdgeCore Switching) (Config-network)#exit
(EdgeCore Switching) (Config-wireless)#ap profile 4
(EdgeCore Switching) (Config-ap-profile)#acl-ip-qos-ratelimit-mode
(EdgeCore Switching) (Config-ap-profile)#radio 1
(EdgeCore Switching) (Config-ap-radio)#vap 0
(EdgeCore Switching) (Config-ap-profile-vap)#network 21
(EdgeCore Switching) (Config-ap-profile-vap)#
```

acl-ip-list

This command adds a rule to an IP ACL list.

IP Access Control Lists (ACL) allow network managers to define classification actions and rules for specific ports (UDP/TCP). ACLs are composed of access control entries (ACE), or rules, that consist of filters that determine traffic classifications. These rules are matched sequentially against a packet. When packet meets the match criteria of a rule, the specific rule action (permit or deny) is taken, and the additional rules are not checked for a match. For example, a network administrator can define an ACL rule that says port number 20 can receive TCP packets. However, if a UDP packet is received then the packet is dropped.

This command must be used in conjunction with the acl-ip-name-create command.

Format `acl-ip-list {dst-ipaddr} {dst-ipmask} {src-ipaddr} {src-ipmask} {dst-port} {src-port} {action} {protocol} {policy-name}`

Mode Wireless Config

Term	*Definition*
dst-ipaddr	The destination port IP address in the packet to compare to the IP address in the packet header.
dst-ipmask	The destination IP wildcard mask (in the second field) to compare to the IP address in the packet header. Wild card masks determine which bits in the IP address are used and which bits are ignored. A wild card mask of 255.255.255.255 indicate that no bit is important. Wild card masking of ACLs operates differently from a subnet mask. A wild card 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 zeros (0's) for the bit positions that are not used. In contrast, a wildcard mask has zeros (0's) in the bit positions that must be checked. A 1 in the bit position of the ACL mask indicates the corresponding bit can be ignored. The field is required when you configure a destination IP address.

Term	*Definition*
src-ipaddr	The source port IP address in the packet to compare to the IP address in the packet header.
src-ipmask	The source IP wildcard mask (in the second field) to compare to the IP address in the packet header. Wild card masks determine which bits in the IP address are used and which bits are ignored. A wild card mask of 255.255.255.255 indicate that no bit is important. Wild card masking of ACLs operates differently from a subnet mask. A wild card 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 zeros (0's) for the bit positions that are not used. In contrast, a wildcard mask has zeros (0's) in the bit positions that must be checked. A 1 in the bit position of the ACL mask indicates the corresponding bit can be ignored. The field is required when you configure a source IP address.
dst-port	The TCP/UDP destination port to match in the packet header. Range: 0-65535
src-port	The TCP/UDP source port to match in the packet header. Range: 0-65535
action	The action to take when a packet or frame matches the criteria in the rule. Range: 0-1, where "0" means deny and "1" means permit. When you select deny, the rule blocks all traffic that meets the rule criteria from entering or exiting the AP (depending on the ACL direction you select). Traffic that does not meet the criteria is forwarded unless this rule is the final rule. Because there is an implicit deny all rule at the end of every ACL, traffic that is not explicitly permitted is dropped When you select permit, the rule allows all traffic that meets the rule criteria to enter or exit the AP (depending on the ACL direction you select). Traffic that does not meet the criteria is dropped.
protocol	Select the Protocol field to use an L3 or L4 protocol match condition based on the value of the IP Protocol field in IPv4 packets. Range: 0-4, 0 (IP), 1 (ICMP), 2 (IGMP), 3 (TCP), 4 (UDP)
policy-name	Select the Policy to configure with the new rule. The policy name can include 1 to 31 alphanumeric characters and the following special characters: hyphen, underscore, backslash and colon. If spaces are used, enclose the name in double quotes.

Example: The following shows an example of the command.

```
(EdgeCore Switching) (Config-wireless)# acl-ip-list 1.1.1.1 255.255.255.0 2.2.2.2 0.0.0.0 20 21 1 3
RD
<cr>    Press Enter to execute the command.
```

no acl-ip-list

The no version of this command removes a rule from an IP ACL list.

Format `no acl-ip-list {dst-ipaddr} {dst-ipmask} {src-ipaddr} {src-ipmask} {dst-port} {src-port} {action} {protocol} {policy-name}`

Mode Wireless Config

For a description of the terms used for no version of this command refer to the acl-ip-list command/

acl-ip-name-create

This command creates an ACL table's name for an IP-ACL policy.

Format `acl-ip-name-create {ip-acl-name}`

Mode Wireless Config

Term	*Definition*
ip-acl-name	Enter the name that identifies the ACL. The ACL name can include 1 to 31 alphanumeric characters and the following special characters: hyphen, underscore, backslash and colon. If spaces are used, enclose the name in double quotes.

ip-acl-policy

This command selects the Policy to be configured with the new rule.

Format `ip-acl-policy {ip-acl}`

Mode Network Config

Term	*Definition*
ip-acl	Enter the name that identifies the IP ACL policy. The policy name can include 1 to 31 alphanumeric characters and the following special characters: hyphen, underscore, backslash and colon. If spaces are used, enclose the name in double quotes.

acl-ip-qos-ratelimit-mode

This command enables IP ACL and QoS Rate Limit modes.

Format `acl-ip-qos-ratelimit-mode`

Mode AP Profile Config

Example: The following shows an example of the command.

```
(EdgeCore Switching) (Config)#wireless
(EdgeCore Switching) (Config-wireless)#ap profile 4
(EdgeCore Switching) (Config-ap-profile)#acl-ip-qos-ratelimit-mode
<cr>    Press Enter to execute the command.
```

no acl-ip-qos-ratelimit-mode

The no version of this command disables IP ACL and QoS Rate Limit modes.

Format `no acl-ip-qos-ratelimit-`

Mode AP Profile Config

WIFI Scheduler Commands

The Radio and VAP Scheduler allows you to automatically enable or disable VAPs and radios based on configured time intervals. This can help reduce power consumption and increase security. For example, the scheduler can be configured so that radios to operate only during the office working hours. Another use case is to allow access to VAPs for wireless clients only during a specific time of the day.

Each rule specifies the start time, end time and day or days of the week the radio or VAP can be operational. The rules are periodic in nature and are repeated every week.

Up to 16 rules are grouped together to form a scheduling profile. Any two periodic rules time entries belonging to the same profile must not overlap. The time granularity for the schedules is one minute. The UAP supports up to 16 profiles.

Use the show show wireless ap profile command to display the WIFI Scheduler settings.

The following example shows how to configure a WIFI access schedule for specified client to client traffic.

```
(EdgeCore Switching) (Config-wireless)#wifi-scheduler admin
(EdgeCore Switching) (Config-wireless)#wifi-scheduler profile-name a3
(EdgeCore Switching) (Config-wireless)#wifi-scheduler profile-rule a3 08 00 17 0  0 daily
(EdgeCore Switching) (Config-wireless)#
```

wifi-scheduler admin-status

This command enables the scheduler.

Default	Disabled
Format	`wifi-scheduler admin-status`
Mode	Wireless Config

no wifi-scheduler admin-status

This no version of this command disables the scheduler.

Default	Disabled
Format	`no wifi-scheduler admin-status`
Mode	Wireless Config

wifi-scheduler profile-name

This command configures a WiFi Scheduler profile name.

Format	`wifi-scheduler profile-name {name}`
Mode	Wireless Config

Term	*Definition*
name	A Scheduler profile that can be associated with a VAP or Radio. Scheduler rules can be associated with a named scheduler profile. You can define up to 16 scheduler profile names. By default, no profiles are created. The profile name can be up to 32 alphanumeric characters.

no wifi-scheduler profile-name

This no version of this command removes a WiFi Scheduler profile name.

Format `no wifi-scheduler profile-name {name}`

Mode Wireless Config

Term	*Definition*
name	A Scheduler profile that can be associated with a VAP or Radio. Scheduler rules can be associated with a named scheduler profile. You can define up to 16 scheduler profile names. The profile name can be up to 32 alphanumeric characters.

wifi-scheduler profile-rule

This command configures a WiFi Scheduler profile rule.

Format `wifi-scheduler profile-rule {name} {start-hour} {start-minute} {end-hour} {end-minute} {days}`

Mode Wireless Config

Term	*Definition*
name	The name of a profile to associated with the desired rule. The profile name can be up to 32 alphanumeric characters.
start-hour	The hour when the radio or VAP will be operationally enabled. Range: 00-23 in 24-hour format. The default is 00 hour.
start-minute	The minute when the radio or VAP will be operationally enabled. Range: 00-59. The default is 00 minutes.
end-hour	The hour when the radio or VAP will be operationally disabled. Range: 00-23 in 24-hour format. The default is 00 hour.
end-minute	The minute when the radio or VAP will be operationally disabled. Range: 00-59. The default is 00 minutes.
days	Options include the day of the week. Range is: **daily**, **weekday** (Monday to Friday), **weekend** (Saturday and Sunday), **monday**, **tuesday**, **wednesday**, **thursday**, **friday**, **saturday**, **sunday**. The default is **daily**.

Example: The following shows an example of the command.

```
(EdgeCore Switching) (Config-)#wireless
(EdgeCore Switching) (Config-wireless)#network 21
(EdgeCore Switching) (Config-network)#ip-acl-policy RD
(EdgeCore Switching) (Config-network)#exit
(EdgeCore Switching) (Config-wireless)#wifi-scheduler profile-rule RD 08 30 17 30 daily
<cr>    Press Enter to execute the command.
```

wifi-scheduler profile-rule-id

This command edits an WiFi Scheduler profile rule.

Format `wifi-scheduler profile-rule-id {name} {rule} {start-minute} {end-hour} {end-minute} {days}`

Mode Wireless Config

Term	*Definition*
name	The name of a profile to associated with the desired rule. The profile name can be up to 32 alphanumeric characters.
rule	The profile rule ID to edit. Range: 0-15.
start-hour	The hour when the radio or VAP will be operationally enabled. Range: 00-23 in 24-hour format. The default is 00 hour.
start-minute	The minute when the radio or VAP will be operationally enabled. Range: 00-59. The default is 00 minutes.
end-hour	The hour when the radio or VAP will be operationally disabled. Range: 00-23 in 24-hour format. The default is 00 hour.
end-minute	The minute when the radio or VAP will be operationally disabled. Range: 00-59. The default is 00 minutes.
days	Options include the day of the week. Range is: **daily**, **weekday** (Monday to Friday), **weekend** (Saturday and Sunday), **monday**, **tuesday**, **wednesday**, **thursday**, **friday**, **saturday**, **sunday**. The default is **daily**.

Example: The following shows an example of the command.

```
(EdgeCore Switching) (Config-wireless)#wifi-scheduler profile-rule RD 09 00 18 00 daily
<cr>    Press Enter to execute the command.
```

wifi-scheduler profile-association

This command a WiFi Scheduler profile to associate with a radio/network.

Format `wifi-scheduler profile-association {name}`

Mode Network Config

Term	*Definition*
name	The name of a profile to associated with the currently configured radio/network. The profile name can be up to 32 alphanumeric characters.

Example: The following shows an example of this command.

```
(EdgeCore Switching) (Config-wireless)#
(EdgeCore Switching) (Config-wireless)#network 20
(EdgeCore Switching) (Config-network)#wifi-scheduler profile-association RD
(EdgeCore Switching) (Config-network)#exit
(EdgeCore Switching) (Config-wireless)#ap profile 1
(EdgeCore Switching) (Config-ap-profile)#radio 1
(EdgeCore Switching) (Config-ap-radio)#wifi-scheduler profile-association RD
(EdgeCore Switching) (Config-ap-radio)#exit
(EdgeCore Switching) (Config-ap-profile)#radio 2
(EdgeCore Switching) (Config-ap-radio)#wifi-scheduler profile-association RD
(EdgeCore Switching) (Config-ap-radio)#end
(EdgeCore Switching)#show wireless ap profile 1
AP Profile ID................................ 1
Profile Name................................. Default
Hardware Type................................ 8 - ECW7220-L AP Dual Radio anac      /bgn
Disconnected AP Data Forwarding Mode.......... Disable
Disconnected AP Management Mode............... Enable
Band Steering Mode........................... Disable
AP Load Balance Mode......................... Disable
AP Load Balance Policy....................... Disable
Wired Network Detection VLAN ID.............. 1
AeroScout Engine Protocol Support............. Disable
Profile Status............................... Associated
Valid APs Configured......................... 2
Managed APs Configured....................... 1

Scheduler Profile Associated with Radio Table (RadioId / ProfileId - ProfileName)
--------------------------------------------------------------------------------
1 / 1 - "RD"
2 / 1 - "RD"

Scheduler Profile Associated with VAP Table (RadioId - VapId / ProfileId - ProfileName)
----------------------------------------------------------------------------------------
1 - 0 / * No profile can be applied to 1st vap
1 - 1 / 0 - No profile applied
1 - 2 / 0 - No profile applied
1 - 3 / 0 - No profile applied
1 - 4 / 0 - No profile applied
1 - 5 / 0 - No profile applied
...
```

Rate Limit Commands

Each rate limit policy is a set of up to 10 rules applied to traffic sent from a wireless client or to be received by a wireless client. Each rule specifies whether the contents of a given field should be used to permit or deny access to the network. Rules can be based on various criteria and may apply to one ore more fields within a packet, such as the source or destination IP address, the source or destination MAC address, the source or destination L4 port, or the protocol carried in the packet.

Use the acl-ip-qos-ratelimit-mode command to enable QoS Rate Limiting.

The show show wireless ap profile command to does not display the QoS Rate Limit settings for this release. (Use the web to WLAN > WLAN Configuration > Gloal > Rate Limit tab to view the QoS Rate Limit settings)

The following example shows how to configure a QoS rate limit and assign it to a radio and VAP.

```
(EdgeCore Switching) (Config-)#wireless
(EdgeCore Switching) (Config-wireless)#rate-limit 100000 192.168.5.0 255.255.255.0 192.168.6.0
255.255.255.0 21 21 11:22:33:44:55:66 ff:ff:ff:ff:ff:00 11:22:33:44:55:66 ff:ff:ff:ff:ff:00 3 turtle 1
1 0 0 0
(EdgeCore Switching) (Config-wireless)#network 21
(EdgeCore Switching) (Config-network)#rate-limit-policy turtle
(EdgeCore Switching) (Config-network)#exit
(EdgeCore Switching) (Config-wireless)#ap profile 4
(EdgeCore Switching) (Config-ap-profile)#acl-ip-qos-ratelimit-mode
(EdgeCore Switching) (Config-ap-profile)#radio 1
(EdgeCore Switching) (Config-ap-radio)#vap 0
(EdgeCore Switching) (Config-ap-profile-vap)#network 21
(EdgeCore Switching) (Config-ap-profile-vap)#
```

rate-limit

This command adds a rule to the QoS rate limit policy.

Format `rate-limit {rate} {dst-ipaddr} {dst-ipmask} {src-ipaddr} {src-ipmask} {dst-port} {src-port} (dst-mac} (dst-mac-mask} (src-mac} (src-mac-mask} (protocol} (policy-name} (vlan-enable} (rate-limit-vlan-id} (service-type} (service-priority} (ip-tos-mask}`

Mode Wireless Config

Term	*Definition*
rate	Enter the maximum allowed transmission rate between the AP and the wireless client in Kbps. The valid range is 0-1363148800 bps. A non-zero configured value is rounded down to the nearest 64 Kbps value for use in the AP, but to no less than 64 Kbps. A value of 0 means that the bandwidth maximum limit is not enforced.
dst-ipaddr	The destination port IP address in the packet to compare to the IP address in the packet header.

Term	*Definition*
dst-ipmask	The destination IP wildcard mask (in the second field) to compare to the IP address in the packet header. Wild card masks determine which bits in the IP address are used and which bits are ignored. A wild card mask of 255.255.255.255 indicate that no bit is important. Wild card masking of ACLs operates differently from a subnet mask. A wild card 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 zeros (0's) for the bit positions that are not used. In contrast, a wildcard mask has zeros (0's) in the bit positions that must be checked. A 1 in the bit position of the ACL mask indicates the corresponding bit can be ignored. The field is required when you configure a destination IP address.
src-ipaddr	The source port IP address in the packet to compare to the IP address in the Source MAC field of the packet header.
src-ipmask	The source IP wildcard mask (in the second field) to compare to the IP address in the packet header. Wild card masks determine which bits in the IP address are used and which bits are ignored. A wild card mask of 255.255.255.255 indicate that no bit is important. Wild card masking of ACLs operates differently from a subnet mask. A wild card 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 zeros (0's) for the bit positions that are not used. In contrast, a wildcard mask has zeros (0's) in the bit positions that must be checked. A 1 in the bit position of the ACL mask indicates the corresponding bit can be ignored. The field is required when you configure a source IP address.
dst-port	The TCP/UDP destination port to match in the packet header.
src-port	The TCP/UDP source port to match in the packet header.
dst-mac	The destination port MAC address in the packet to compare to the MAC address in Destination MAC field of the packet header.
dst-mac-mask	Enter the destination MAC address mask specifying which bits in the destination MAC address to compare to the MAC address in the packet header. A 0 indicates that the address bit is significant, and an f indicates that the address bit is to be ignored. A MAC mask of 00:00:00:00:00:00 matches a single MAC address.
src-mac	The source port MAC address in the packet to compare to the MAC address in Source MAC field of the packet header.
src-mac-mask	Enter the source MAC address mask specifying which bits in the source MAC address to compare to the MAC address in the packet header. A 0 indicates that the address bit is significant, and an f indicates that the address bit is to be ignored. A MAC mask of 00:00:00:00:00:00 matches a single MAC address.
protocol	The protocol type to match within the IP Protocol field in the IP packet header. You can specify one of the following keywords: IP, ICMP, IGMP, TCP, or UDP.
policy-name	The rate limit policy that defines the list of rate limit rules that can be associated with a VAP or Radio. Rules are associated with a named scheduler profile. You can define up to 32 scheduler profile names. By default, no profiles are created. The policy name can include 1 to 31 alphanumeric characters and the following special characters: hyphen, underscore, backslash and colon. If spaces are include, enclose them in double quotes.
vlan-enable	Enter "1" to compare the VLAN ID specified by this policy against an Ethernet frame. Enter "0" to disable this feature.
rate-limit-vlan-id	Enter the VLAN ID to compare against an Ethernet frame. This field is located in the first/only 802.1Q VLAN tag.
service-type	Select this field and enter an 802.1p user priority to compare against an Ethernet frame.

Term	*Definition*
service-priority	To use IP DSCP as a match criteria, select a DSCP keyword from the list. Use this field to enter IP DSCP List (0-63) or IP Precedence value (0-7) or **ip-tos-bits** in IP TOS Bits Protocol (0-255) depending on the specified service type. When setting **ip-tos-bits,** enter a value to match against the packet's Type of Service bits in the IP header. The IP TOS field in a packet is defined as all eight bits of the Service Type octet in the IP header. The TOS Bits value is a two-digit hexadecimal number from 00 to ff. The high-order three bits represent the IP precedence value. The high-order six bits represent the IP Differentiated Services Code Point (DSCP) value.
ip-tos-mask	Enter an IP TOS mask value to identify the bit positions in the TOS Bits value that are used for comparison against the IP TOS field in a packet. The TOS Mask value is a two-digit hexadecimal number from 00 to ff, representing an inverted (i.e. wildcard) mask. The zero-valued bits in the TOS Mask denote the bit positions in the TOS Bits value that are used for comparison against the IP TOS field of 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 TOS Bits value of a 0 and a TOS Mask of 00. This is an optional configuration. To comply with the syntax for this command, you must enter the dummy value "0" in the last field of the ip-tos-mask when service-priority is set to 0 (IP DSCP) or 1 (IP Precedence).

Example: The following shows an example of the command.

```
(EdgeCore Switching) (Config-)#wireless
(EdgeCore Switching) (Config-wireless)#rate-limit 100000 192.168.5.0 255.255.255.0 192.168.6.0
255.255.255.0 21 21 11:22:33:44:55:66 ff:ff:ff:ff:ff:00 11:22:33:44:55:66 ff:ff:ff:ff:ff:00 3 turtle
1 1 0 0 0
<cr>    Press Enter to execute the command.
```

no rate-limit

The no version of this command removes a rule from the QoS rate limit policy.

Format `no rate-limit {rate} {dst-ipaddr} {dst-ipmask} {src-ipaddr} {src-ipmask} {dst-port} {src-port} (dst-mac} (dst-mac-mask} (src-mac} (src-mac-mask} (protocol} (policy-name} (vlan-enable} (rate-limit-vlan-id} (service-type} (service-priority} (ip-tos-mask}`

Mode Wireless Config

For a description of the terms used for no version of this command refer to the rate-limit command/

rate-limit-name-create

This command creates a policy name for the rate limit policy.

Format `rate-limit-name-create {name}`

Mode Wireless Config

Term	*Definition*
name	The rate limit policy defines the list of rate limit rules that can be associated with a VAP or Radio configuration. Rules are associated with a named scheduler policy. You can define up to 32 scheduler policy names. By default, no policies are created. The policy name can include 1 to 31 alphanumeric characters and the following special characters: hyphen, underscore, backslash and colon. If spaces are include, enclose them in double quotes.

no rate-limit-name-create

The no version of this command removes a policy name used for rate limiting.

Format `no rate-limit-name-create {name}`

Mode Wireless Config

For a description of the terms used for no version of this command refer to the rate-limit-name-create command.

rate-limit-policy

This command selects the name of a rate limit policy.

Format `rate-limit-policy {name}`

Mode Network Config

Term	*Definition*
name	The rate limit policy defines the list of rate limit rules that can be associated with a VAP or Radio configuration. Rules are associated with a named scheduler policy. You can define up to 32 scheduler policy names. By default, no policies are created. The policy name can include 1 to 31 alphanumeric characters and the following special characters: hyphen, underscore, backslash and colon. If spaces are include, enclose them in double quotes.

no rate-limit-policy

The no version of this command removes a policy name used for rate limiting.

Format `no rate-limit-name-create {name}`

Mode Wireless Config

For a description of the terms used for no version of this command refer to the rate-limit-policy command.

Edge-Core AP Commands

This section describes the commands you use to download code versions to Edge-Core APs.

accton-ap download-mode

This command selects the protocol for downloading code updates to Edge-Core APs.

Format `accton-ap {0-9} download-mode {ftp | tftp}`

Mode Wireless Config

Term	*Definition*
0-8	An index number indicating the Edge-Core AP type.
ftp	Keyword to select FTP protocol download mode.
tftp	Keyword to select TFTP protocol download mode.

accton-ap filename

This command sets the file name of software code updates to Edge-Core APs.

Format `accton-ap {0-8} filename` *name*

Mode Wireless Config

Term	*Definition*
0-8	An index number indicating the Edge-Core AP type.
name	The name of the code file to download.

accton-ap reset-mode

This command selects the type of reboot for specified Edge-Core AP.

Format `accton-ap {0-10} reset-mode board`

Mode Wireless Config

Term	*Definition*
0-10	An index number indicating the Edge-Core AP type.
board	Restarts the AP using the current saved configuration.

accton-ap server-ip

This command sets the IP address of the host server where download files are located.

Format `accton-ap {0-10} server-ip {`*ipaddr*`}`

Mode Wireless Config

Term	*Definition*
0-10	An index number indicating the Edge-Core AP type.
ipaddr	The IP address of the host where the upgrade file is located. The host must have an FTP or TFTP server installed and running.

accton-ap software

This command sets the software version of the code on the host server.

Format `accton-ap {0-10} software {name}`

Mode Wireless Config

Term	*Definition*
0-10	An index number indicating the Edge-Core AP type.
name	A string of up to 32 characters that identify the software version on the server. If the code on the AP is a different version, the AP will upgrade itself automatically.

accton-ap username

This command sets the FTP user name on the host server.

Format `accton-ap {0-10} username {name}`

Mode Wireless Config

Term	*Definition*
0-10	An index number indicating the Edge-Core AP type.
name	A string of up to 32 characters that is the FTP user name required for download.

accton-ap userpassword

This command sets the FTP password on the host server.

Format `accton-ap {0-10} userpassword {name}`

Mode Wireless Config

Term	*Definition*
0-10	An index number indicating the Edge-Core AP type.
name	A string of up to 64 characters that is the FTP password required for download.

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 {1-500}`

Mode Wireless Config

Parameter	*Description*
1–500	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 {1-500}`

Mode Wireless Config

Example: The following shows an example of the command.

```
(EdgeCore Switching) (Config-wireless)# ap profile 1
(EdgeCore Switching) (Config-ap-profile)#
```

If the profile is in use:

```
(EdgeCore Switching) (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

disconnected-ap forwarding-mode

This command enables the Disconnected AP Data Forwarding Mode so that the managed AP allows clients that are already associated to continue forwarding traffic if the AP loses connection with the wireless switch.

Default Disabled

Format `disconnected-ap forwarding-mode`

Mode AP Profile Config

no disconnected-ap forwarding-mode

This command resets the Disconnected AP Data Forwarding Mode to the default value.

Format `disconnected-ap forwarding-mode`

Mode AP Profile Config

disconnected-ap management-mode

This command enables the Disconnected AP Management Mode so that the managed AP allows CLI, web, and SNMP access to the AP management interface if the AP loses connection with the wireless switch.

Default Enabled

Format `disconnected-ap forwarding-mode`

Mode AP Profile Config

no disconnected-ap management-mode

This command resets the Disconnected AP Management Mode to the default value.

Format `disconnected-ap forwarding-mode`

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 {0-20}`

Mode AP Profile Config

Parameter	*Description*
0–20	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

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.

```
(EdgeCore Switching) (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.

```
(EdgeCore Switching) (Config-ap-profile)#  no vlan
<cr>    Press Enter to execute the command.
```

acl-ip-mode

This command enables ACL filtering of IP addresses denied access to the network.

Default	Disabled
Format	`acl-ip-mode`
Mode	AP Profile Config

no acl-ip-mode

The `no` version of this command disables IP ACL filtering.

Format	`no acl-ip-mode`
Mode	AP Profile Config

acl-ip-list

This command configures a list of IP addresses denied access to the network.

Default	None configured
Format	`acl-ip-list {ipaddr}`
Mode	AP Profile Config

Parameter	*Description*
ipaddr	A wireless client IP address.

no acl-ip-list

The `no` version of this command removes all IP addresses from the list.

Format	`no acl-ip-list`
Mode	AP Profile Config

dhcp-relay-ip

This command configures the global DHCP relay server IP address for the wireless network.

Default 0.0.0.0
Format `dhcp-relay-ip {ipaddr}`
Mode AP Profile Config

Parameter	*Description*
ipaddr	The IP address of the DHCP relay server.

no dhcp-relay-ip

The `no` version of this command restores the default setting for the DHCP relay server IP address.

Format `no dhcp-relay-ip`
Mode AP Profile Config

multiple-vlan

This command configures multiple VLAN IDs for OAP9112CA units. Up to 32 VLAN IDs can be specified for OAP9112CA units only.

Default none
Format `multiple-vlan {vlanid1 [,vlanid2,vlanid3, .....vlanid32]}`
Mode AP Profile Config

Parameter	*Description*
vlanid1....vlanid32	Enter up to 32 VLAN ID numbers separated by commas.

no multiple-vlan

The `no` version of this command removes all multiple VLAN settings.

Format `no multiple-vlan`
Mode AP Profile Config

schedule-reboot-interval

This command configures an AP reboot interval time in seconds.

Default 0 (disabled)
Format `schedule-reboot-interval {0, 30-259200}`
Mode AP Profile Config

Parameter	*Description*
0, 30-259200	Enter the interval in seconds, or enter zero to disable the scheduled reboot.

no schedule-reboot-interval

The `no` version of this command disables the scheduled reboot.

Format `no schedule-reboot-interval`
Mode AP Profile Config

tun-switch-ip

This command configures the primary controller switch IP address for a CAPWAP data tunnel.

Default 0.0.0.0
Format `tun-switch-ip {ipaddr}`
Mode AP Profile Config

Parameter	*Description*
ipaddr	The IP address of the primary controller switch.

no tun-switch-ip

The `no` version of this command restores the default setting for the primary controller switch IP address.

Format `no tun-switch-ip`
Mode AP Profile Config

tun-switch-port

This command configures the primary controller switch UDP port number for a CAPWAP data tunnel.

Default 30000
Format `tun-switch-port {1024-65535}`
Mode AP Profile Config

Parameter	*Description*
1024-65535	The UDP port number for the primary controller switch.

no tun-switch-port

The `no` version of this command restores the default setting for the primary controller switch UDP port.

Format `no tun-switch-port`
Mode AP Profile Config

tun-switch-2th-ip

This command configures the secondary controller switch IP address for a CAPWAP data tunnel.

Default 0.0.0.0
Format `tun-switch-2th-ip {ipaddr}`
Mode AP Profile Config

Parameter	*Description*
ipaddr	The IP address of the secondary controller switch.

no tun-switch-2th-ip

The `no` version of this command restores the default setting for the secondary controller switch IP address.

Format `no tun-switch-2th-ip`
Mode AP Profile Config

tun-switch-2th-port

This command configures the secondary controller switch UDP port number for a CAPWAP data tunnel.

Default 30000
Format `tun-switch-2th-port {1024-65535}`
Mode AP Profile Config

Parameter	*Description*
1024-65535	The UDP port number for the secondary controller switch.

no tun-switch-2th-port

The `no` version of this command restores the default setting for the secondary controller switch UDP port.

Format `no tun-switch-2th-port`
Mode AP Profile Config

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 {1-500} {1-500}`
Mode Wireless Config

Parameter	*Description*
1–500	Source AP Profile ID.
1–500	Destination AP Profile ID.

Example: The following shows an example of the command.

If the destination AP Profile is associated with Managed APs:

```
(EdgeCore Switching) (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 {1-500}`

Mode Privileged EXEC

Parameter	*Description*
1–500	AP Profile ID.

Example: The following shows an example of the command.

If the profile is associated with WS Managed APs:

```
(EdgeCore Switching) (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.

```
(EdgeCore Switching) (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 [{1-500} [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.

Field	*Description*
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.
Valid APs Configured	The number of APs using a specific profile ID stored in AP's local database.
Managed APs Configured	The number of APs using specific profile ID and operating in managed state.

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

```
(EdgeCore Switching) #show wireless ap profile 1

AP Profile ID................................ 1
Profile Name................................. Default
Hardware Type................................ 0 - Any
Disconnected AP Data Forwarding Mode........... Disable
Disconnected AP Management Mode.............. Enable
Band Steering Mode........................... Disable
AP Load Balance Mode......................... Disable
Wired Network Detection VLAN ID.............. 0
AeroScout Engine Protocol Support............ Disable
Profile Status............................... Configured
Valid APs Configured......................... 0
Managed APs Configured....................... 2
```

show wireless ap profile radio auto-eligible

This command displays each channel included in the automatic channel assignment process.

Format `show wireless ap profile [{1-500} [radio [{1-2}]]] auto-eligible`

Mode Privileged EXEC

Field	*Description*
AP Profile ID	Existing AP profile ID.
Profile Name	A descriptive name for the corresponding AP profile ID.
Radio	AP profile radio interface.
Mode	Indicates the physical layer technology for the radio.
Supported Channels	This field displays the channels that are supported for the configured radio mode.

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

```
(EdgeCore Switching) #show wireless ap profile 1 radio 1 auto-eligible

AP Profile ID................................ 1
```

```
Profile Name..................................... Default
Radio............................................ 1 - 802.11b/g/n
Mode............................................. 802.11b/g/n

Supported Channels (* = Auto Eligible)
-----------------------------------------------

    1*    2     3     4     5     6*    7     8
    9    10    11*
```

show wireless ap profile radio mcs-indices

This command displays the Modulation and Coding Scheme (MCS) index values supported by the radio.

Format `show wireless ap profile [{1-500} [radio [{1-2}]]] mcs-indices`

Mode Privileged EXEC

Field	*Description*
AP Profile ID	Existing AP profile ID.
Profile Name	A descriptive name for the corresponding AP profile ID.
Radio	AP profile radio interface.
Mode	Indicates the physical layer technology for the radio.
Supported MCS Indices	This field displays the MCS index values supported by the radio.

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

```
(EdgeCore Switching) #show wireless ap profile 1 radio 1 mcs-indices

AP Profile ID.................................... 1
Profile Name..................................... Default
Radio............................................ 1 - 802.11b/g/n
Mode............................................. 802.11b/g/n

Supported MCS Indices
-----------------------------------------------
     0     1     2     3     4     5     6     7
     8     9    10    11    12    13    14    15
    16    17    18    19    20    21    22    23
```

show wireless ap profile radio vap

This command displays AP profile information about the specified virtual access point.

Format `show wireless ap profile [{1-500} [radio [{1-2}]]] vap [0-15]`

Mode Privileged EXEC

Field	*Description*
AP Profile ID	Existing AP profile ID.
Radio	AP profile radio interface.
Mode	Indicates whether or not the VAP is enabled or disabled. VAPs are always configured, but are only sending beacons and accepting clients when they are Enabled.
Network	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.

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

```
(EdgeCore Switching) #show wireless ap profile 1 radio 1 mcs-indices

AP Profile ID.............................. 1
Radio...................................... 1 - 802.11b/g/n
Mode....................................... 802.11b/g/n
VAP ID..................................... 1
Mode....................................... Disable
Network.................................... 2-ManagedSSID_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 | a-n | bg-n | 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.
a-n	Indicates 802.11a/n as physical mode.
bg-n	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:

```
(EdgeCore Switching) (Config-ap-profile)#radio 1
(EdgeCore Switching) (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

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 100

Format `max-clients {1-100}`

Mode AP Profile Radio Config

Parameter	*Description*
1–100	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 {1-100}`

Mode AP Profile Radio Config

Parameter	*Description*
1–100	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

Parameter	*Description*
value	A valid rate based on radio mode.

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

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

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

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

frame-no-ack

This command configures the radio so that it does not acknowledge frames with QosNoAck as the service class value.

Default	Disabled
Format	`frame-no-ack`
Mode	AP Profile Radio Config

no frame-no-ack

The `no` version of this command resets the acknowledgment to the default value.

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 {1-500} [radio {1-2} [[rates [{basic | supported}]]`
Mode	Privileged EXEC

Parameter	*Description*
AP Profile ID	AP profile ID.
Profile Name	Descriptive name associated with the AP Profile ID.
Radio	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).
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.
Enable Broadcast/ Multicast Rate Limiting	Indicates if broadcast and multicast traffic rate limiting is enabled on the radio.

Parameter	*Description*
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.
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.
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.
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.

Parameter	*Description*
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.
Radio Resource Measurement	Indicates if Radio Resource Measurement (RRM) should be enabled for this radio, if supported.
Multicast Rate Limit (pkts/s)	The rate at which the radio transmits the multicast frames

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

```
(EdgeCore Switching) # show wireless ap profile 1 radio 1

AP Profile ID.................................. 1
Profile Name................................... Default
Radio.......................................... 1 - 802.11b/g/n
Status......................................... On
Mode........................................... 802.11b/g/n
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
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
Maximum Receive Lifetime....................... 512
Maximum Clients................................ 256
Automatic Channel Adjustment................... Disable
Automatic Power Adjustment..................... Disable
Default Power (%).............................. 100
Load Balancing................................. Disable
Load Utilization (%)........................... 60
Station Isolation.............................. Disable
Channel Bandwidth.............................. 20 MHz
Primary Channel................................ Upper
Protection..................................... Auto
Short Guard Interval........................... Enabled
STBC Mode...................................... Enabled
Multicast Transmit Rate........................ Auto
Automatic Power Save Delivery Mode............. Enabled
No Ack......................................... Enabled
Radio Resource Measurement..................... Enable
Local Power Constraint (dBm)................... 0
Multicast Rate Limit (pkts/s).................. 0
```

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.

```
(EdgeCore Switching) #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.

```
(EdgeCore Switching) #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 edca template

This command allows you to select a pre-defined QoS template to apply to the AP profile. If you use the `custom` keyword, you can change the AP and station parameters. If you use the voice or Defaults keywords, the switch will use the pre-defined settings for the template you select, and you will not be able to configure QoS settings with the `qos ap-edca` or `qos station-edca` commands.

Default Custom

Format `qos edca template {custom | default | voice}`

Mode AP Profile Radio Config

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. The range is 1, 3, 7, 15, 31, 63, 127, 255, 511 or 1023 milliseconds.
cwmax-time	Maximum contention window value in milliseconds. The range is 1, 3, 7, 15, 31, 63, 127, 255, 511 or 1023 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. The range is 1, 3, 7, 15, 31, 63, 127, 255, 511 or 1023 milliseconds.
cwmax-time	Maximum Contention Window value in milliseconds. The range is 1, 3, 7, 15, 31, 63, 127, 255, 511 or 1023 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 {1-500} 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	AP profile radio interface.
Mode	The configured physical mode for the radio.
Template	A pre-defined QoS template applied to the AP profile.
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.

Parameter	*Description*
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...................................... 1 - 802.11b/g/n
Mode....................................... 802.11b/g/n
Template................................... Custom
WMM Mode................................... Disable

AP EDCA Configuration
---------------------
QoS                        Minimum            Maximum        Maximum
Queues          AIFS   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...................................... 1 - 802.11b/g/n
Mode....................................... 802.11b/g/n
Template................................... Custom
WMM Mode................................... Disable

Station EDCA Configuration
--------------------------
QoS                        Minimum            Maximum         Tx Op
Queues          AIFS   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 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 {1-256}`

Mode AP Profile VAP Config

Parameter	*Description*
1–256	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 {1-4} {url}`

Mode Privileged EXEC

Parameter	*Description*
1–4	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 {1-20}`

Mode Privileged EXEC

Parameter	*Description*
1–6	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 {1-4}] [macaddr]`

Mode Privileged EXEC

Parameter	*Description*
1–4	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.

```
(EdgeCore Switching) #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 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`

Mode Privileged EXEC

Example: The following shows an example of the command.

```
(EdgeCore Switching) #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).
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.

Field	*Description*
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.
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.
L2 Tunnel Interface	The designation for a layer 2 tunnel interface – a logical point-to-point link that carries encapsulated packets.
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:

```
(EdgeCore Switching) #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:

```
(EdgeCore Switching) #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

(EdgeCore Switching) #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....................................... Edge-Core
Protocol Version................................ 2
Software Version................................ D.05.22.1
Hardware Type................................... 14 - ECW5110-L Dual Radio
                                                 a/b/g/n
Serial Number................................... H05167353
Part Number..................................... ECW5110-L
Discovery Reason................................ L2 Poll Received
Authenticated Clients........................... 0
L2 Tunnel Interface............................. 7/2
System Up Time.................................. 0d:00:02:43
Age............................................. 0d:00:00:02
```

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.

Field	*Description*
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.
Transmit Power	If the radio is operational, the current transmit power for the radio.
Auth. Clients	Total count of clients in the associated client database with an *Authenticated* status.
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.
Channel Bandwidth	If the radio is operational, the current channel bandwidth in use.
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.
Authenticated Clients	Total number of clients in the associated client database with an *Authenticated* status.
Total Neighbors	Total number of neighbors (both APs and clients) that can be seen by this radio in its RF area.
WLAN Utilization	Indicates the total network utilization for the physical radio. This value is based on radio statistics.
Radio Resource Measurement	Indicates if Radio Resource Measurement (RRM) is enabled for this radio, if supported.

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:

```
(EdgeCore Switching) #show wireless ap radio status

    MAC Address                                    Transmit   Auth.
 (*) Peer Managed       Location        Radio Channel Power (%) Clients
------------------ -------------------- ----- ------- --------- -------
 70:72:CF:89:01:40 factory              1     1       100       1
                                        2     36      100       0
*B8:9B:C9:FD:B0:80 ECW5110-L
                                        1     11      100       0
                                        2     40      100       0
```

On the switch that is not acting as a Cluster Controller, the summary command displays entries in the following format:

```
(EdgeCore Switching) #show wireless ap radio status
                                                    Transmit   Auth.
    MAC Address         Location        Radio Channel Power (%) Clients
----------------- -------------------- ----- ------- --------- -------
 70:72:CF:89:01:40                     1     0       0         0
                                       2     0       0         0
 B8:9B:C9:FD:B0:80 ECW5110-L
                                       1     11      100       0
                                       2     40      100       0

(EdgeCore Switching) #show wireless ap 00:01:01:02:01:01 radio 1 status

MAC address..................................... B8:9B:C9:FD:B0:80
Location........................................ FirstFloor
Radio........................................... 1 - 802.11b/g/n
Supported Channels.............................. 5, 6, 7, 8, 9, 10, 11
Channel......................................... 11
Channel Bandwidth............................... 40 MHz
Fixed Channel Indicator......................... No
Manual Channel Adjustment Status................ Not Started
Transmit Power.................................. 100 %
Fixed Power Indicator........................... No
Manual Power Adjustment Status.................. Not Started
Authenticated Clients........................... 0
Total Neighbors................................. 0
WLAN Utilization................................ 0
Radio Resource Measurement...................... Enabled
(EdgeCore Switching) #
```

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.

```
(EdgeCore Switching) #show wireless ap 70:72:CF:89:01:40 radio 1 channel status

Manual Channel Adjustment Status.............. Success
```

```
Channel..................................... 1
```

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.
Manual Power Adjustment Status	Indicates the current state of a manual request to change the power setting on this radio.
Transmit Power	If the radio is operational, the current transmit power for the radio.

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 Authentications	Indicates the total number of clients currently associated and authenticated to the VAP.

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

```
(EdgeCore Switching) #show wireless ap 00:01:01:02:01:01 radio 1 vap status

MAC address..................................... 70:72:CF:89:01:40
Location........................................ factory
Radio........................................... 1 - 802.11b/g/n

                                                    Client
VAP ID   VAP MAC Address            SSID            Auth.
------ ------------------ ----------------------- ------
0      70:72:CF:89:01:40   GuestNetwork            1
1      70:72:CF:89:01:41   ManagedSSID_2           0
2      70:72:CF:89:01:42   ManagedSSID_3           0
3      70:72:CF:89:01:43   ManagedSSID_4           0
4      70:72:CF:89:01:44   ManagedSSID_5           0
5      70:72:CF:89:01:45   ManagedSSID_6           0
6      70:72:CF:89:01:46   ManagedSSID_7           0
7      70:72:CF:89:01:47   ManagedSSID_8           0
8      70:72:CF:89:01:48   ManagedSSID_9           0
9      70:72:CF:89:01:49   ManagedSSID_10          0
10     70:72:CF:89:01:4A   ManagedSSID_11          0
11     70:72:CF:89:01:4B   ManagedSSID_12          0
12     70:72:CF:89:01:4C   ManagedSSID_13          0
13     70:72:CF:89:01:4D   ManagedSSID_14          0
14     70:72:CF:89:01:4E   ManagedSSID_15          0
15     70:72:CF:89:01:4F   ManagedSSID_16          0

(EdgeCore Switching) #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 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).

Field	*Description*
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*. • Unknown ("-"): The AP is detected in the network but is not classified as a threat by the threat detection algorithms.
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.

```
(EdgeCore Switching) #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
----------------- ------------------------ ---- --------------- ---------------
00:13:F7:DC:EB:98 SF-AP2                   51   Managed         0d:00:23:13
00:22:2D:4D:7B:42 A1000015-1872            59   Managed         0d:00:18:10
00:AE:AE:01:36:20 980029-3176-Tallac       49   Managed         0d:01:23:14
```

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.

Field	*Description*
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.

```
(EdgeCore Switching) #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 Packets Transmitted	Total packets transmitted by the AP on the wireless network.
WLAN Bytes Received	Total bytes received 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 Packets Transmit Dropped	Total transmitted packets discarded by the AP on the wireless network.
WLAN Bytes Receive Dropped	Total receive bytes discarded by the AP on the wireless network.
WLAN Bytes Transmit Dropped	Total transmitted bytes discarded by the AP on the wireless network.
Ethernet Packets Received	Total packets received by the AP on the wired network.
Ethernet Packets Transmitted	Total packets transmitted by the AP on the wired network.
Ethernet Bytes Received	Total bytes transmitted by the AP on the wired network.
Ethernet Bytes Transmitted	Total bytes transmitted by the AP on the wired network.
Ethernet Multicast Packets Received	Total multicast packets received 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.
Central L2 Tunnel Bytes Received	Total bytes received by the AP L2 tunnels on the wired network.
Central L2 Tunnel Packets Received	Total packets by the AP L2 tunnels on the wired network.
Central L2 Tunnel Multicast Packets Received	Total multicast packets by the AP L2 tunnels on the wired network.
Central L2 Tunnel Bytes Transmitted	Total bytes transmitted by the AP L2 tunnels on the wired network.
Central L2 Tunnel Packets Transmitted	Total packets transmitted by the AP L2 tunnels on the wired network.
Central L2 Tunnel Multicast Packets Transmitted	Total multicast packets transmitted by the AP L2 tunnels 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.

```
(EdgeCore Switching) #show wireless ap b8:9b:c9:fd:b0:80 statistics

MAC address..................................... B8:9B:C9:FD:B0:80
Location........................................ ECW5110-L
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
Central L2 Tunnel Bytes Received................ 0
Central L2 Tunnel Packets Received.............. 0
Central L2 Tunnel Multicast Packets Received... 0
Central L2 Tunnel Bytes Transmitted............. 0
Central L2 Tunnel Packets Transmitted........... 0
Central L2 Tunnel Multicast Packets Transmitt.. 0
ARP Reqs Converted from Bcast to Ucast......... 0
Filtered ARP Requests........................... 0
Broadcasted ARP Requests........................ 0

(EdgeCore Switching) #
```

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.

Field	*Description*
WLAN Packets Transmitted	Total packets discarded by the AP prior to transmission on this radio interface.
WLAN Bytes Received	Total bytes received 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 Packets Transmit Dropped	Total transmitted packets discarded by the AP on this radio interface.
WLAN Bytes Receive Dropped	Total receive bytes discarded by the AP on this radio interface.
WLAN Bytes Transmit Dropped	Total transmitted bytes discarded by the AP on this radio interface.
Fragments Received	Count of successfully received MPDU frames of type data or management.
Fragments Transmitted	Count of acknowledged MPDU with an individual address or an MPDU with a multicast address of type Data or Management.
Multicast Frames Transmitted	Count of successfully transmitted MSDU frames where the multicast bit is set in the destination MAC address.
Multicast Frames Received	Count of MSDU frames received with the multicast bit set in the destination MAC address.
Duplicate Frame Count	Number of times a frame is received and the Sequence Control field indicates it is a duplicate.
Failed Transmit 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.
Transmit 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.
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.
FCS Error Count	Count of FCS errors detected in a received MPDU frame.
Frames Transmitted	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.

```
(EdgeCore Switching) #show wireless ap b8:9b:c9:fd:b0:80 radio 1 statistics

MAC address..................................... B8:9B:C9:FD:B0:80
```

```
Location..................................... ECW5110-L
Radio........................................ 1 - 802.11b/g/n
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 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.

Field	*Description*
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.

```
(EdgeCore Switching) #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 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 1 File Name	The AP image type 1 filename on the TFTP server.
Image 1 File Path	The AP image type 1 file path on the TFTP server.
Image 2 File Name	The AP image type 2 filename on the TFTP server.
Image 2 File Path	The AP image type 2 file path on the TFTP server.
Image 3 File Name	The AP image type 3 filename on the TFTP server.
Image 3 File Path	The AP image type 3 file path on the TFTP server.
Image 4 File Name	The AP image type 4 filename on the TFTP server.
Image 4 File Path	The AP image type 4 file path on the TFTP server.

Field	*Description*
Image 5 File Name	The AP image type 5 filename on the TFTP server.
Image 5 File Path	The AP image type 5 file path 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.

```
(EdgeCore Switching) #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
image 3 File Name..............................
image 3 File Path..............................
image 4 File Name..............................
image 4 File Path..............................
image 5 File Name..............................
image 5 File Path..............................
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.

```
(EdgeCore 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.

```
(EdgeCore Switching) #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.

(EdgeCore Switching) #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:

```
(EdgeCore Switching) #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:

(EdgeCore Switching) #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


(EdgeCore Switching) #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....................................... Accton
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.

```
(EdgeCore Switching) #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.
SSID	Service Set ID of the network, this is broadcast in the detected beacon frame.
Physical Mode	Indicates the 802.11 mode being used on the AP.
Channel	Transmit channel of the 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*.

Field	*Description*
Age	Time in seconds since this AP was last detected in an RF scan.
The following parameters are displayed only in the detailed status:	
OUI	Vendor name for the MAC address.
BSSID	Basic Service Set Identifier advertised by the AP in the beacon frames.
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).
Transmit Rate	Indicates the rate at which the AP is currently transmitting data.
Beacon Interval	Beacon interval for the neighbor AP network.
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.
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 is 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.
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.
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.

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

```
(EdgeCore Switching) #show wireless ap rf-scan status

                                                    Physical
   MAC Address          SSID           Mode     Chan     Status         Age
----------------- ----------------  ----------- ---- ------------ -------------
00:01:01:02:01:03 Network3          802.11g     6    Managed      0d:00:27:51
00:01:01:02:03:02 Network2          802.11g     6    Managed      0d:00:01:07
00:33:01:02:01:83 Lobby             802.11g     6    Unknown      0d:00:00:06
```

```
(EdgeCore Switching) #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
BSSID........................................... B8:9B:C9:FD:B0:80
Physical Mode................................... 802.11g
Channel......................................... 1
Status.......................................... Rogue
Initial Status.................................. Rogue
Transmit Rate (Mpbs)............................ 1 Mbps
Beacon Interval (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

(EdgeCore Switching) #
```

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.
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.

```
(EdgeCore Switching) #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.

```
(EdgeCore Switching) # 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|ap macaddr| ssid name| vap macaddr]`

Mode Privileged EXEC

Parameter	*Description*
macaddr	Client MAC address.
ap	Disassociates all clients from the specified managed AP.
ssid	Disassociates all clients from the specified SSID.
vap	Disassociates all clients from the specified VAP interface.

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.
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 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.
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.
Channel	Indicates the operating channel for the client association.
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.
VLAN	If the client is on a VAP using VLAN data forwarding mode, indicates the current assigned VLAN.
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:

```
(EdgeCore Switching) #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
```

On the switch that is not acting as a Cluster Controller the summary command displays entries in the following format:

```
(EdgeCore Switching) #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
```

Example: The following shows CLI display output for a particular MAC address:

```
(EdgeCore Switching) #show wireless client 00:14:6c:59:d1:99 status

MAC address..................................... 00:14:6C:59:D1:99
Detected IP Address............................. 192.168.0.2
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
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
```

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:

```
(EdgeCore Switching) #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

(EdgeCore Switching) #
```

On the switch that is not acting as a Cluster Controller the summary command displays entries in the following format:

```
(EdgeCore Switching) #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 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.
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.

```
(EdgeCore Switching) #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
```

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 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.
AP MAC Address	Indicates the Ethernet MAC address for the managed AP which detected the client.
Location	The configured descriptive location for the managed AP.

Field	*Description*
Radio	The radio interface on the AP.
Client MAC Address	The Ethernet address of client station.

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

```
(EdgeCore Switching) #show wireless vap client status

 VAP MAC Address   AP MAC Address        Location      Radio Client MAC Address
----------------- ----------------- ------------------ ----- ------------------
70:72:CF:89:01:40 70:72:CF:89:01:40 factory            1     00:25:D3:8F:F9:95
```

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.

```
(EdgeCore Switching) #show wireless ssid client status

                                    Client
             SSID                 MAC Address
------------------------------ -----------------
Network2                       00:01:01:16:01:01
                               00:01:01:20:01:01
                               00:01:01:22:01:01
Network3                       00:01:01:10:01:01
                               00:01:01:14:01:01
```

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:

```
 (EdgeCore Switching) #show wireless switch client status

Switch IP Address  Client MAC Address
-----------------  ------------------
192.168.37.60      00.0F.B5.86.93.95
                   00:14:C2:0C:47:6D
192.168.37.61      00.0F.B5.86.93.85
                   00:14:C2:0C:47:1D

(EdgeCore Switching) #show wireless switch 192.168.37.60 client status

Switch IP Address  Client MAC Address
-----------------  ------------------
192.168.37.60      00.0F.B5.86.93.95
                   00:14:C2:0C:47:6D
```

On the switch that is not acting as a Cluster Controller the summary command displays entries in the following format:

```
(EdgeCore Switching) #show wireless switch client status

Switch IP Address  Client MAC Address
-----------------  ------------------
 192.168.37.61     00.0F.B5.86.93.85
                   00:14:C2:0C:47:1D

(EdgeCore Switching) #show wireless switch 192.168.37.60 client status
Error! Only Cluster Controller can display the peer switch associated client status.
```

```
(EdgeCore Switching) #show wireless switch 192.168.37.61 client status

Switch IP Address  Client MAC Address
-----------------  ------------------
192.168.37.61      00.0F.B5.86.93.85
                   00:14:C2:0C:47:1D
```

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 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 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.

```
(EdgeCore Switching) #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

(EdgeCore Switching) #
```

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-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 - 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 - fake managed AP/ managed SSID	Enable or disable rogue reporting for fake managed APs 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.

```
(EdgeCore Switching) # 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 - no SSID in the beacon..... 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 - fake managed AP / managed SSID..... Enable
Rogue - unmanaged AP on a wired network..... Enable
Rogue - unexpected WDS devices..... Enable
Rogue detected trap interval..... 300 seconds
```

```
Wired network detection interval.............. 60 seconds
AP De-Authentication Attack................... Disable
```

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.

```
(EdgeCore Switching) # 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.

```
(EdgeCore Switching) # 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 {60-3600}`

Mode Wireless Config

Parameter	*Description*
60–3600	Interval in seconds between transmissions of the trap. The range is 60–3600 seconds.

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.

```
(EdgeCore Switching) # wids-security client rogue-det-trap-interval 60  ?
<cr>    Press Enter to execute the command.

(EdgeCore Switching) # 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

wireless 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 `wireless detected-client [`*macaddr*`] ack-rogue`

Mode Privileged EXEC

Parameter	*Description*
macaddr	The Ethernet address of the client.

clear wireless detected-client non-auth

Use this command to delete the non-authenticated client entry for all the entries present in the database. If the client is authenticated, then this command has no effect.

Format `clear wireless detected-client non-auth`

Mode Privileged EXEC

Example: The following shows an example of the command.

```
clear wireless detected-client non-auth
Are you sure you want to clear the entire detected client list? (y/n) y
Wireless detected-client list cleared.
```

clear wireless detected-client roam-history

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 `clear wireless detected-client [macaddr] roam-history`

Mode Privileged EXEC

Example: The following shows an example of the command.

```
clear wireless detected-client roam-history
Are you sure you want to clear the roam-history for all the detected clients? (y/n) y
Roam history purged for all detected-clients.
```

clear wireless detected-client preauth-history

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 `clear wireless detected-client [macaddr] preauth-history`

Mode Privileged EXEC

Example: The following shows an example of the command.

```
wireless detected-client preauth-history-purge
Are you sure you want to clear the pre-auth-history for all the detected clients? (y/n) y
Pre-auth history purged for all detected-clients.
```

show wireless client detected-client preauth-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 preauth-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.)
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.

```
(EdgeCore Switching) # show wireless client detected-client preauth-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

(EdgeCore Switching) # 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 Accton 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.
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.

```
(EdgeCore Switching) # 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

(EdgeCore Switching) # show wireless client 00:02:BB:00:0A:01 detected-client roam-history

Client MAC Address.......................... 00:25:D3:8F:F9:95

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.
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.

```
(EdgeCore Switching) # 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.
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.

Field	*Description*
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.

```
(EdgeCore Switching) # 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

(EdgeCore Switching) # show wireless client 00:13:46:C1:78:67 detected-client status
MAC address..................................... 00:13:46:C1:78:67
OUI............................................. Accton
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 OUI database	If client MAC address is not in the Known OUI Client database, then report the client as Rogue.
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.

Field	*Description*
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.

```
(EdgeCore Switching) # show wireless wids-security client

Rogue detected trap interval.................. 300 seconds
Rogue-Not in OUI database..................... Disable
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.

```
(EdgeCore Switching) # show wireless wids-security client rogue-test-descriptions

WIDSCLIENTROGUE1.........Client not listed in the Known Clients database
WIDSCLIENTROGUE2.........Client exceeds configured rate for auth msgs
WIDSCLIENTROGUE3.........Client exceeds configured rate for probe msgs
WIDSCLIENTROGUE0.........Client exceeds configured rate for de-auth msgs
WIDSCLIENTROGUE5.........Client exceeds max failing authentications
WIDSCLIENTROGUE6.........Known client authenticated with unknown AP
WIDSCLIENTROGUE7.........Client OUI not in the OUI Database
```

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

mutual-auth-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-auth-mode`
Mode	Wireless Config

no mutual-auth-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-auth-mode`
Mode	Wireless Config

Example: The following shows an example of the command.

```
(Switch wireless) #mutual-auth-mode
Enabling Mutual Authentication Mode might result in network traffic disruption. Are you sure you want
to continue? (y/n) y
```

re-provision-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-provision-unmanaged`
Mode	Wireless Config

no re-provision-unmanaged

The `no` version of the command disables re-provisioning for APs in the network when in unmanaged mode.

Format	`no re-provision-unmanaged`
Mode	Wireless Config

Example: The following shows an example of the command.

```
(Switch wireless) #re-provision-unmanaged
This configuration will be sent to all switches in cluster. Are you sure you want to continue? (y/n) y
```

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.
```

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.

```
(EdgeCore Switching) #wireless certificate-generate
```

show wireless ap provisioning status

This command displays status information for entries in ap provisioning database. This command displays summary status for all entries in the ap provisioning in the database.

Format `show wireless ap provisioning status`

Mode Privileged EXEC

Field	*Description*
macaddr	The Ethernet address of the client.
IP Address	IP Address of the AP.
Primary Switch IP	IP Address of the primary provisioned switch as reported by the AP.
Backup Switch IP	IP Address of the backup provisioned switch as reported by the AP.
Provisioning Status	Status of the most recently issued AP provisioning command.
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.

```
(EdgeCore Switching) # 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
```

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

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.

```
(EdgeCore Switching)(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.

```
(EdgeCore Switching)(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.

```
(EdgeCore Switching) #show wireless device-location

Measurement System.............................. Metric
RF-Scan Location Report......................... Enable
RF-Scan Location 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.

```
(EdgeCore Switching) #show wireless device-location building

Building  Building Description  Number of Floors  Number of APs
--------  --------------------  ----------------  -------------
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.

```
(EdgeCore Switching) #show wireless device-location building 1

Building Number.............. 1
Building Description.......... building-1
Number of Floors.............. 6
Number of APs................. 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,

```
(EdgeCore Switching) #show wireless device-location building floor

Building/                       Number
Floor       Floor Description   of APs
---------   ------------------ ----------
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,

```
(EdgeCore Switching) #show wireless device-location building 1 floor

                                Number
Floor       Floor Description   of APs
---------   ------------------ ----------
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,

```
(EdgeCore Switching) #show wireless device-location building 1 floor 1

Building Number.............. 1
Building Description.......... building-1
Floor ........................ 1
Floor Description.............. floor-1
Number of APs................. 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.

```
(EdgeCore Switching) #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.

```
(EdgeCore Switching) #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.

```
(EdgeCore Switching) #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.

Field	*Description*
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.

```
(EdgeCore Switching) # show wireless device-location ap triangulation status-all

                                Building/   Detected XY   Last
Device MAC                      Floor       Coordinate    Computation
Address            Device Type  Number      (Meters)      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.

```
(EdgeCore Switching) # 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.

```
(EdgeCore Switching) # 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.

```
(EdgeCore Switching) # show wireless device-location client triangulation status-all

                                    Building/   Detected XY   Last
Device MAC                          Floor       Coordinate    Computation
Address            Device Type      Number      (Meters)      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.

```
(EdgeCore Switching) # 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

(EdgeCore Switching) # 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.

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.

```
(EdgeCore Switching) #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.

```
(EdgeCore Switching) #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.

```
(EdgeCore Switching) #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.

```
(EdgeCore Switching) #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

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.

```
(EdgeCore Switching) #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.

```
(EdgeCore Switching) #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

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.
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.
Time since device-location triggered	The time the device location search was started.
Number of Locator APs	Number of managed APs that were used for locating the target device.
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.

```
(EdgeCore Switching) #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
Time since device-location triggered...... 0d:00:00:03
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

(EdgeCore Switching) #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

(EdgeCore Switching) #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

(EdgeCore Switching) #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.

```
(EdgeCore Switching) #show wireless device-location floor-status

                    Number of                           Circle
Building/  Device    Detecting  Solution    (X,Y)        Radius   Sigma
Floor      Found     APs        Type        (Meters)     (Meters) (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.

```
(EdgeCore Switching) #show wireless device-location floor-status building 6

                    Number of                           Circle
Building/  Device    Detecting  Solution    (X,Y)        Radius   Sigma
Floor      Found     APs        Type        (Meters)     (Meters) (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.

```
(EdgeCore Switching) #show wireless device-location floor-status
building 2 floor 4

Device Found.................................. Found
Number of Detecting APs....................... 2
Solution Type................................. Point Solution
X-axis Coordinate............................. 126 Meters
Y-axis Coordinate............................. -161 Meters
Circle Radius................................. 0 Meters
Sigma......................................... 5 Meters
```

Section 8: Quality of Service Commands

This chapter describes the Quality of Service (QoS) commands available in the EWS4502/EWS4606 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.

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

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

Appendix A: Log Messages

This chapter lists common log messages that are provided by EWS4502/EWS4606, 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 10: BSP Log Messages

Component	*Message*	*Cause*
BSP	Event(0xaaaaaaaa)	Switch has restarted.
BSP	Starting code...	BSP initialization complete, starting EWS4502/EWS4606 application.

Table 11: NIM Log Messages

Component	*Message*	*Cause*
NIM	NIM: L7_ATTACH out of order for interface unit x slot x port x	Interface creation out of order.
NIM	NIM: Failed to find interface at unit x slot x port x for event(x)	There is no mapping between the USP and Interface number.
NIM	NIM: L7_DETACH out of order for interface unit x slot x port x	Interface creation out of order.
NIM	NIM: L7_DELETE out of order for interface unit x slot x port x	Interface creation out of order.

Table 11: NIM Log Messages (Cont.)

Component	*Message*	*Cause*
NIM	NIM: event(x),intf(x),component(x), in wrong phase	An event was issued to NIM during the wrong configuration phase (probably Phase 1, 2, or WMU).
NIM	NIM: Failed to notify users of interface change	Event was not propagated to the system.
NIM	NIM: failed to send message to NIM message Queue.	NIM message queue full or non-existent.
NIM	NIM: Failed to notify the components of L7_CREATE event	Interface not created.
NIM	NIM: Attempted event (x), on USP x.x.x before phase 3	A component issued an interface event during the wrong initialization phase.
NIM	NIM: incorrect phase for operation	An API call was made during the wrong initialization phase.
NIM	NIM: Component(x) failed on event(x) for interface	A component responded with a fail indication for an interface event.
NIM	NIM: Timeout event(x), interface remainingMask = xxxx	A component did not respond before the NIM timeout occurred.

Table 12: 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 13: System Log Messages

Component	*Message*	*Cause*
SYSTEM	Configuration file hawk.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 13: 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 14: Trap Mgr Log Message

Component	Message	Cause
Trap Mgr	Link Up/Down: unit/slot/port	An interface changed link state.

Table 15: 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 16: 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 17: RADIUS Log Messages

Component	*Message*	*Cause*
RADIUS	RADIUS: Invalid data length - xxx	The RADIUS Client received an invalid message from the server.
RADIUS	RADIUS: Failed to send the request	A problem communicating with the RADIUS server.
RADIUS	RADIUS: Failed to send all of the request	A problem communicating with the RADIUS server during transmit.
RADIUS	RADIUS: Could not get the Task Sync semaphore!	Resource issue with RADIUS Client service.
RADIUS	RADIUS: Buffer is too small for response processing	RADIUS Client attempted to build a response larger than resources allow.
RADIUS	RADIUS: Could not allocate accounting requestInfo	Resource issue with RADIUS Client service.
RADIUS	RADIUS: Could not allocate requestInfo	Resource issue with RADIUS Client service.
RADIUS	RADIUS: osapiSocketRecvFrom returned error	Error while attempting to read data from the RADIUS server.
RADIUS	RADIUS: Accounting-Response failed to validate, id = xxx	The RADIUS Client received an invalid message from the server.
RADIUS	RADIUS: User (xxx) needs to respond for challenge	An unexpected challenge was received for a configured user.
RADIUS	RADIUS: Could not allocate a buffer for the packet	Resource issue with RADIUS Client service.
RADIUS	RADIUS: Access-Challenge failed to validate, id = xxx	The RADIUS Client received an invalid message from the server.
RADIUS	RADIUS: Failed to validate Message-Authenticator, id = xxx	The RADIUS Client received an invalid message from the server.
RADIUS	RADIUS: Access-Accept failed to validate, id = xxx	The RADIUS Client received an invalid message from the server.

Table 17: RADIUS Log Messages (Cont.)

Component	Message	Cause
RADIUS	RADIUS: Invalid packet length – xxx	The RADIUS Client received an invalid message from the server.
RADIUS	RADIUS: Response is missing Message-Authenticator, id = xxx	The RADIUS Client received an invalid message from the server.
RADIUS	RADIUS: Server address doesn't match configured server	RADIUS Client received a server response from an unconfigured server.

Table 18: LLDP Log Message

Component	Message	Cause
LLDP	lldpTask(): invalid message type:xx. xxxxxx:xx	Unsupported LLDP packet received.

Table 19: 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 20: 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 21: SNMP Log Message

Component	*Message*	*Cause*
SNMP	EDB Callback: Unit Join: x.	A new unit has joined the stack.

Table 22: 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 23: 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 24: 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 25: 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 26: 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 27: 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 28: 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 29: 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 30: 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 31: 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 32: MFDB Log Message

Component	*Message*	*Cause*
MFDB	mfdbTreeEntryUpdate: entry does not exist	Trying to update a non existing entry.

Table 33: 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.
802.1Q	Problem deleting data for VLAN %d	Failed to delete VLAN ID from the VLAN database.

Table 33: 802.1Q Log Messages (Cont.)

Component	Message	Cause
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 34: 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 35: 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.

QoS

Table 36: 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 37: 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 38: 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

Table 39: 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.

Technologies

Table 40: Accton Error Messages

Component	Message	Cause
Accton	Invalid USP unit = x, slot = x, port = x	A port was not able to be translated correctly during the receive.
Accton	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.
Accton	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.

Table 40: Accton Error Messages (Cont.)

Component	*Message*	*Cause*
Accton	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.
Accton	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.
Accton	ACL x not found in internal table	Attempting to delete a non-existent ACL.
Accton	ACL internal table overflow	Attempting to add an ACL to a full table.
Accton	In hapiBroadQosCosQueueConfig, Failed to configure minimum bandwidth. Available bandwidth x	Attempting to configure the bandwidth beyond it's capabilities.
Accton	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.
Accton	USL: failed to sync ipmc table on unit = x	Either the transport failed or the message was dropped.
Accton	usl_task_ipmc_msg_send(): failed to send with x	Either the transport failed or the message was dropped.
Accton	USL: No available entries in the STG table	The Spanning Tree Group table is full in USL.
Accton	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.
Accton	USL: A Trunk doesn't exist in USL	Attempting to modify a Trunk that doesn't exist.
Accton	USL: A Trunk being created by bcmx already existed in USL	Possible synchronization issue between the application, hardware, and sync layer.
Accton	USL: A Trunk being destroyed doesn't exist in USL	Possible synchronization issue between the application, hardware, and sync layer.
Accton	USL: A Trunk being set doesn't exist in USL	Possible synchronization issue between the application, hardware, and sync layer.
Accton	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.
Accton	USL: Mcast entry not found on a join	Possible synchronization issue between the application, hardware, and sync layer.
Accton	USL: Mcast entry not found on a leave	Possible synchronization issue between the application, hardware, and sync layer.
Accton	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.
Accton	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.

Table 40: Accton Error Messages (Cont.)

Component	Message	Cause
Accton	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.
Accton	Invalid LAG id x	Possible synchronization issue between the BCM driver and HAPI.
Accton	Invalid uport calculated from the BCM uport bcmx_l2_addr->lport = x	Uport not valid from BCM driver.
Accton	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.
Accton	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.
Accton	Unable to Insert host H	Host H could not be inserted in hardware host table. A retry will be issued.
Accton	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.
Accton	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.
Accton	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.
Accton	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.
Accton	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.
Accton	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 41: 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.

Table 41: OSAPI VxWorks Log Messages (Cont.)

Component	*Message*	*Cause*
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.
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 42: Linux BSP Log Message

Component	*Message*	*Cause*
Linux BSP	rc = 10	Second message logged at bootup, right after *Starting code…. Always* logged.

Table 43: 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.

Table 43: OSAPI Linux Log Messages (Cont.)

Component	*Message*	*Cause*
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.
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