Consolidated Platform Command Reference, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)

First Published: April 12, 2013

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-29471-01

CONTENTS

Preface

This preface contains the following topics:

Document Conventions

This document uses the following conventions:

Convention	Description
^ or Ctrl	Both the ^ symbol and Ctrl represent the Control (Ctrl) key on a keyboard. For example, the key combination **^D** or **Ctrl-D** means that you hold down the Control key while you press the D key. (Keys are indicated in capital letters but are not case sensitive.)
bold font	Commands and keywords and user-entered text appear in **bold** font.
Italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
`Courier font`	Terminal sessions and information the system displays appear in `courier` font.
`Bold Courier font`	Bold Courier font indicates text that the user must enter.
[x]	Elements in square brackets are optional.
...	An ellipsis (three consecutive nonbolded periods without spaces) after a syntax element indicates that the element can be repeated.
|	A vertical line, called a pipe, indicates a choice within a set of keywords or arguments.

Convention	Description
[x | y]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
{x | y}	Required alternative keywords are grouped in braces and separated by vertical bars.
[x {y | z}]	Nested set of square brackets or braces indicate optional or required choices within optional or required elements. Braces and a vertical bar within square brackets indicate a required choice within an optional element.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
< >	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Reader Alert Conventions

This document uses the following conventions for reader alerts:

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

Tip Means *the following information will help you solve a problem.*

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Timesaver Means *the described action saves time.* You can save time by performing the action described in the paragraph.

Warning **Means *reader be warned.* In this situation, you might perform an action that could result in bodily injury.**

Related Documentation

Note Before installing or upgrading the controller, refer to the controller release notes.

- Cisco 5700 Series Wireless Controller documentation, located at:

  http://www.cisco.com/go/wlc5700_sw

- Cisco Validated Designs documents, located at:

  http://www.cisco.com/go/designzone

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

Using the Command-Line Interface

This module contains the following topics:

Information About Using the Command-Line Interface

This section describes the Cisco IOS command-line interface (CLI) and how to use it.

Command Modes

The Cisco IOS user interface is divided into many different modes. The commands available to you depend on which mode you are currently in. Enter a question mark (?) at the system prompt to obtain a list of commands available for each command mode.

When you start a session using Telnet, SSH, or console on the controller, you begin in user mode, often called user EXEC mode. Only a limited subset of the commands are available in user EXEC mode. For example, most of the user EXEC commands are one-time commands, such as **show** commands, which show the current configuration status, and **clear** commands, which clear counters or interfaces. The user EXEC commands are not saved when the controller reboots.

To have access to all commands, you must enter privileged EXEC mode. Normally, you must enter a password to enter privileged EXEC mode. From this mode, you can enter any privileged EXEC command or enter global configuration mode.

Using the configuration modes (global, interface, and line), you can make changes to the running configuration. If you save the configuration, these commands are stored and used when the controller reboots. To access the various configuration modes, you must start at global configuration mode. From global configuration mode, you can enter interface configuration mode and line configuration mode.

This table describes the main command modes, how to access each one, the prompt you see in that mode, and how to exit the mode.

Table 1: Command Mode Summary

Mode	Access Method	Prompt	Exit Method	About This Mode
User EXEC	Begin a session using Telnet, SSH, or console.	`Controller>`	Enter **logout** or **quit**.	Use this mode to • Change terminal settings. • Perform basic tests. • Display system information.
Privileged EXEC	While in user EXEC mode, enter the **enable** command.	`Controller#`	Enter **disable** to exit.	Use this mode to verify commands that you have entered. Use a password to protect access to this mode.
Global configuration	While in privileged EXEC mode, enter the **configure** command.	`Controller(config)#`	To exit to privileged EXEC mode, enter **exit** or **end**, or press **Ctrl-Z**.	Use this mode to configure parameters that apply to the entire controller.
VLAN configuration	While in global configuration mode, enter the **vlan** *vlan-id* command.	`Controller(config-vlan)#`	To exit to global configuration mode, enter the **exit** command. To return to privileged EXEC mode, press **Ctrl-Z** or enter **end**.	Use this mode to configure VLAN parameters. When VTP mode is transparent, you can create extended-range VLANs (VLAN IDs greater than 1005) and save configurations in the controller startup configuration file.
Interface configuration	While in global configuration mode, enter the **interface** command (with a specific interface).	`Controller(config-if)#`	To exit to global configuration mode, enter **exit**. To return to privileged EXEC mode, press **Ctrl-Z** or enter **end**.	Use this mode to configure parameters for the Ethernet ports.

Mode	Access Method	Prompt	Exit Method	About This Mode
Line configuration	While in global configuration mode, specify a line with the **line vty** or **line console** command.	`Controller(config-line)#`	To exit to global configuration mode, enter **exit**. To return to privileged EXEC mode, press **Ctrl-Z** or enter **end**.	Use this mode to configure parameters for the terminal line.

Using the Help System

You can enter a question mark (?) at the system prompt to display a list of commands available for each command mode. You can also obtain a list of associated keywords and arguments for any command.

SUMMARY STEPS

1. **help**
2. *abbreviated-command-entry* **?**
3. *abbreviated-command-entry* <Tab>
4. **?**
5. *command* **?**
6. *command keyword* **?**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**help** **Example:** `Controller# help`	Obtains a brief description of the help system in any command mode.

Step 2	*abbreviated-command-entry* **?**
	
	Example:
	`Controller# di?`
	`dir disable disconnect`
		Obtains a list of commands that begin with a particular character string.

Step 3	*abbreviated-command-entry* <Tab>
	
	Example:
	`Controller# sh conf<tab>`
	`Controller# show configuration`
		Completes a partial command name.

	Command or Action	Purpose
Step 4	**?** **Example:** `Controller> ?`	Lists all commands available for a particular command mode.
Step 5	*command* **?** **Example:** `Controller> show ?`	Lists the associated keywords for a command.

Step 6	*command keyword* **?**
	
	Example:
	`Controller(config)# cdp holdtime ?`
	`  <10-255> Length of time (in sec) that receiver must keep this packet`
		Lists the associated arguments for a keyword.

Understanding Abbreviated Commands

You need to enter only enough characters for the controller to recognize the command as unique.

This example shows how to enter the **show configuration** privileged EXEC command in an abbreviated form:

```
Controller# show conf
```

No and default Forms of Commands

Almost every configuration command also has a **no** form. In general, use the **no** form to disable a feature or function or reverse the action of a command. For example, the **no shutdown** interface configuration command reverses the shutdown of an interface. Use the command without the keyword **no** to reenable a disabled feature or to enable a feature that is disabled by default.

Configuration commands can also have a **default** form. The **default** form of a command returns the command setting to its default. Most commands are disabled by default, so the **default** form is the same as the **no** form. However, some commands are enabled by default and have variables set to certain default values. In these cases, the **default** command enables the command and sets variables to their default values.

CLI Error Messages

This table lists some error messages that you might encounter while using the CLI to configure your controller.

Table 2: Common CLI Error Messages

Error Message	Meaning	How to Get Help
`% Ambiguous command: "show con"`	You did not enter enough characters for your controller to recognize the command.	Reenter the command followed by a question mark (?) with a space between the command and the question mark. The possible keywords that you can enter with the command appear.
`% Incomplete command.`	You did not enter all the keywords or values required by this command.	Reenter the command followed by a question mark (?) with a space between the command and the question mark. The possible keywords that you can enter with the command appear.
`% Invalid input detected at '^' marker.`	You entered the command incorrectly. The caret (^) marks the point of the error.	Enter a question mark (?) to display all the commands that are available in this command mode. The possible keywords that you can enter with the command appear.

Configuration Logging

You can log and view changes to the controller configuration. You can use the Configuration Change Logging and Notification feature to track changes on a per-session and per-user basis. The logger tracks each configuration command that is applied, the user who entered the command, the time that the command was entered, and the parser return code for the command. This feature includes a mechanism for asynchronous notification to registered applications whenever the configuration changes. You can choose to have the notifications sent to the syslog.

Note Only CLI or HTTP changes are logged.

How to Use the CLI to Configure Features

Configuring the Command History

The software provides a history or record of commands that you have entered. The command history feature is particularly useful for recalling long or complex commands or entries, including access lists. You can customize this feature to suit your needs.

Changing the Command History Buffer Size

By default, the controller records ten command lines in its history buffer. You can alter this number for a current terminal session or for all sessions on a particular line. These procedures are optional.

SUMMARY STEPS

1. **terminal history** [**size** *number-of-lines*]
2. **history** [**size** *number-of-lines*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**terminal history** [**size** *number-of-lines*] **Example:** `Controller# terminal history size 200`	Changes the number of command lines that the controller records during the current terminal session in the privileged EXEC mode. You can configure the size from 0 through 256.
Step 2	**history** [**size** *number-of-lines*] **Example:** `Controller(config)# history size 200`	Configures the number of command lines the controller records for all sessions on a particular line in the configuration mode. You can configure the size from 0 through 256.

Recalling Commands

To recall commands from the history buffer, perform one of the actions listed in this table. These actions are optional.

Note The arrow keys function only on ANSI-compatible terminals such as VT100s.

SUMMARY STEPS

1. **Ctrl-P** or use the **up arrow** key
2. **Ctrl-N** or use the **down arrow** key
3. **show history**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**Ctrl-P** or use the **up arrow** key	Recalls commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.

	Command or Action	Purpose
Step 2	**Ctrl-N** or use the **down arrow** key	Returns to more recent commands in the history buffer after recalling commands with **Ctrl-P** or the up arrow key. Repeat the key sequence to recall successively more recent commands.
Step 3	**show history** **Example:** `Controller# show history`	Lists the last several commands that you just entered in privileged EXEC mode. The number of commands that appear is controlled by the setting of the **terminal history** global configuration command and the **history** line configuration command.

Disabling the Command History Feature

The command history feature is automatically enabled. You can disable it for the current terminal session or for the command line. These procedures are optional.

SUMMARY STEPS

1. **terminal no history**
2. **no history**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**terminal no history** **Example:** `Controller# terminal no history`	Disables the feature during the current terminal session in the privileged EXEC mode.
Step 2	**no history** **Example:** `Controller(config)# no history`	Disables command history for the line in the configuration mode.

Enabling and Disabling Editing Features

Although enhanced editing mode is automatically enabled, you can disable it, reenable it, or configure a specific line to have enhanced editing. These procedures are optional.

SUMMARY STEPS

1. **no editing**
2. **terminal editing**
3. **editing**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**no editing** **Example:** `Controller(config)# no editing`	Disables the enhanced editing mode.
Step 2	**terminal editing** **Example:** `Controller# terminal editing`	Reenables the enhanced editing mode for the current terminal session in the privileged EXEC mode.
Step 3	**editing** **Example:** `Controller(config)# editing`	Reconfigures a specific line to have enhanced editing mode.

Editing Commands through Keystrokes

The keystrokes help you to edit the command lines. These keystrokes are optional.

Note The arrow keys function only on ANSI-compatible terminals such as VT100s.

SUMMARY STEPS

1. **Ctrl-B** or use the **left arrow** key
2. **Ctrl-F** or use the **right arrow** key
3. **Ctrl-A**
4. **Ctrl-E**
5. **Esc B**
6. **Esc F**
7. **Ctrl-T**
8. **Ctrl-Y**
9. **Esc Y**
10. **Delete** or **Backspace** key
11. **Ctrl-D**
12. **Ctrl-K**
13. **Ctrl-U** or **Ctrl-X**
14. **Ctrl-W**
15. **Esc D**
16. **Esc C**
17. **Esc L**
18. **Esc U**
19. **Ctrl-V** or **Esc Q**
20. **Return** key
21. **Space** bar
22. **Ctrl-L** or **Ctrl-R**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**Ctrl-B** or use the **left arrow** key	Moves the cursor back one character.
Step 2	**Ctrl-F** or use the **right arrow** key	Moves the cursor forward one character.
Step 3	**Ctrl-A**	Moves the cursor to the beginning of the command line.
Step 4	**Ctrl-E**	Moves the cursor to the end of the command line.
Step 5	**Esc B**	Moves the cursor back one word.
Step 6	**Esc F**	Moves the cursor forward one word.
Step 7	**Ctrl-T**	Transposes the character to the left of the cursor with the character located at the cursor.
Step 8	**Ctrl-Y**	Recalls the most recent entry in the buffer.

	Command or Action	Purpose
		Recall commands from the buffer and paste them in the command line. The controller provides a buffer with the last ten items that you deleted.
Step 9	**Esc Y**	Recalls the next buffer entry. The buffer contains only the last 10 items that you have deleted or cut. If you press **Esc Y** more than ten times, you cycle to the first buffer entry.
Step 10	**Delete** or **Backspace** key	Erases the character to the left of the cursor.
Step 11	**Ctrl-D**	Deletes the character at the cursor.
Step 12	**Ctrl-K**	Deletes all characters from the cursor to the end of the command line.
Step 13	**Ctrl-U** or **Ctrl-X**	Deletes all characters from the cursor to the beginning of the command line.
Step 14	**Ctrl-W**	Deletes the word to the left of the cursor.
Step 15	**Esc D**	Deletes from the cursor to the end of the word.
Step 16	**Esc C**	Capitalizes at the cursor.
Step 17	**Esc L**	Changes the word at the cursor to lowercase.
Step 18	**Esc U**	Capitalizes letters from the cursor to the end of the word.
Step 19	**Ctrl-V** or **Esc Q**	Designates a particular keystroke as an executable command, perhaps as a shortcut.
Step 20	**Return** key	Scrolls down a line or screen on displays that are longer than the terminal screen can display. **Note** The More prompt is used for any output that has more lines than can be displayed on the terminal screen, including **show** command output. You can use the **Return** and **Space** bar keystrokes whenever you see the More prompt.
Step 21	**Space** bar	Scrolls down one screen.
Step 22	**Ctrl-L** or **Ctrl-R**	Redisplays the current command line if the controller suddenly sends a message to your screen.

Editing Command Lines That Wrap

You can use a wraparound feature for commands that extend beyond a single line on the screen. When the cursor reaches the right margin, the command line shifts ten spaces to the left. You cannot see the first ten characters of the line, but you can scroll back and check the syntax at the beginning of the command. The keystroke actions are optional.

To scroll back to the beginning of the command entry, press **Ctrl-B** or the left arrow key repeatedly. You can also press **Ctrl-A** to immediately move to the beginning of the line.

Note The arrow keys function only on ANSI-compatible terminals such as VT100s.

The following example shows how to wrap a command line that extend beyond a single line on the screen.

SUMMARY STEPS

1. **access-list**
2. **Ctrl-A**
3. **Return** key

DETAILED STEPS

	Command or Action	Purpose

Step 1	**access-list**
	
	Example:
	`Controller(config)# access-list 101 permit tcp 10.15.22.25 255.255.255.0 10.15.22.35`
	`Controller(config)# $ 101 permit tcp 10.15.22.25 255.255.255.0 10.15.22.35 255.25`
	`Controller(config)# $t tcp 10.15.22.25 255.255.255.0 131.108.1.20 255.255.255.0 eq`
	`Controller(config)# $15.22.25 255.255.255.0 10.15.22.35 255.255.255.0 eq 45`
		Displays the global configuration command entry that extends beyond one line.
		When the cursor first reaches the end of the line, the line is shifted ten spaces to the left and redisplayed. The dollar sign ($) shows that the line has been scrolled to the left. Each time the cursor reaches the end of the line, the line is again shifted ten spaces to the left.

Step 2	**Ctrl-A** **Example:** `Controller(config)# access-list 101 permit tcp 10.15.22.25 255.255.255.0 10.15.2$`	Checks the complete syntax. The dollar sign ($) appears at the end of the line to show that the line has been scrolled to the right.
Step 3	**Return** key	Execute the commands. The software assumes that you have a terminal screen that is 80 columns wide. If you have a different width, use the **terminal width** privileged EXEC command to set the width of your terminal. Use line wrapping with the command history feature to recall and modify previous complex command entries.

Searching and Filtering Output of show and more Commands

You can search and filter the output for **show** and **more** commands. This is useful when you need to sort through large amounts of output or if you want to exclude output that you do not need to see. Using these commands is optional.

SUMMARY STEPS

1. {**show** | **more**} *command* | {**begin** | **include** | **exclude**} *regular-expression*

DETAILED STEPS

	Command or Action	Purpose
Step 1	{**show**	**more**} *command*	{**begin**	**include**	**exclude**} *regular-expression* **Example:** `Controller# show interfaces	include protocol` `Vlan1 is up, line protocol is up` `Vlan10 is up, line protocol is down` `GigabitEthernet1/0/1 is up, line protocol is down` `GigabitEthernet1/0/2 is up, line protocol is up`	Searches and filters the output. Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain **output** are not displayed, but the lines that contain **output** appear.

Accessing the CLI

You can access the CLI through a console connection, through Telnet, or by using the browser.

Accessing the CLI through a Console Connection or through Telnet

Before you can access the CLI, you must connect a terminal or a PC to the controller console or connect a PC to the Ethernet management port and then power on the controller, as described in the hardware installation guide that shipped with your controller.

If your controller is already configured, you can access the CLI through a local console connection or through a remote Telnet session, but your controller must first be configured for this type of access.

You can use one of these methods to establish a connection with the controller:

- Connect the controller console port to a management station or dial-up modem, or connect the Ethernet management port to a PC. For information about connecting to the console or Ethernet management port, see the controller hardware installation guide.
- Use any Telnet TCP/IP or encrypted Secure Shell (SSH) package from a remote management station. The controller must have network connectivity with the Telnet or SSH client, and the controller must have an enable secret password configured.
    - The controller supports up to 16 simultaneous Telnet sessions. Changes made by one Telnet user are reflected in all other Telnet sessions.
    - The controller supports up to five simultaneous secure SSH sessions.

  After you connect through the console port, through the Ethernet management port, through a Telnet session or through an SSH session, the user EXEC prompt appears on the management station.

PART I

System Management

Cisco 5700 Series System Management Commands

This module contains the following commands:

arp

To display the contents of the Address Resolution Protocol (ARP) table, use the **arp** command in boot loader mode.

arp [*ip_address*]

Syntax Description

ip_address	(Optional) Shows the ARP table or the mapping for a specific IP address.

Command Default

None

Command Modes

Boot loader

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The ARP table contains the IP-address-to-MAC-address mappings.

Examples

This example shows how to display the ARP table:

```
Controller # arp 172.20.136.8
arp'ing 172.20.136.8...
172.20.136.8 is at 00:1b:78:d1:25:ae, via port 0
```

Related Commands

Command	Description
set	Sets the BOOT environment variable to boot a specific image when the BOOT keyword is appended to the command.

boot

To load and boot an executable image and then enter the command-line interface (CLI), use the **boot** command in boot loader mode.

boot [*flag*] *filesystem:/file-url...*

Syntax Description

filesystem:	Alias for a flash file system. Use **flash:** for the system board flash device.
/file-url	(Optional) Path (directory) and name of a bootable image. Separate image names with a semicolon.

Command Default

None

Command Modes

Boot loader

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

When you enter the **boot** command without any arguments, the controller attempts to automatically boot the system by using the information in the BOOT environment variable, if any. If you supply an image name for the *file-url* variable, the **boot** command attempts to boot the specified image.

When you set boot loader **boot** command options, they are executed immediately and apply only to the current boot loader session. These settings are not saved for the next boot operation.

Filenames and directory names are case sensitive.

Examples

This example shows how to boot the controller using the *new-image.bin* image:

```
boot flash:/new-images/new-image.bin
```

After entering this command, you are prompted to start the setup program.

Related Commands

Command	Description
set	Sets the BOOT environment variable to boot a specific image when the **BOOT** keyword is appended to the command.

cat

To display the contents of one or more files, use the **cat** command in boot loader mode.

cat *filesystem:/file-url...*

Syntax Description

filesystem:	Alias for a flash file system. Use **flash:** for the system board flash device.
/file-url	Path (directory) and name of the files to display. Separate each filename with a space.

Command Default

None

Command Modes

Boot loader

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Filenames and directory names are case sensitive.

If you specify a list of files, the contents of each file appears sequentially.

Examples

This example shows how to display the contents of an image file:

```
Controller# cat flash: image_file_name /info
version_suffix: universal-122-xx.SEx
version_directory: image_file_name
image_system_type_id: 0x00000002
image_name: image_file_name.bin
ios_image_file_size: 8919552
total_image_file_size: 11592192
image_feature: IP|LAYER_3|PLUS|MIN_DRAM_MEG=128
image_family: family
stacking_number: 1.34
board_ids: 0x00000068 0x00000069 0x0000006a 0x0000006b
info_end:
```

Related Commands

Command	Description
more	Displays the contents of one or more files.

Command	Description
type	Displays the contents of one or more files.

clear location

To clear a specific radio frequency identification (RFID) tag or all of the RFID tags information in the entire database, use the **clear location** command.

clear location [mac-address *mac-address* |**rfid]**

Syntax Description

mac-address *mac-address*	MAC address of a specific RFID tag.
rfid	Specifies all of the RFID tags in the database.

Command Default

None

Command Modes

User EXEC or privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to clear information about all of the RFID tags in the database:

```
Controller> clear location rfid
```

clear location statistics

To clear radio-frequency identification (RFID) statistics, use the **clear location statistics** command.

clear location statistics

Command Default

None

Command Modes

User EXEC or privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

The following is sample output from the **clear location rfid** command and shows how to clear RFID statistics:

```
Controller> clear location statistics
```

clear nmsp statistics

To clear the Network Mobility Services Protocol (NMSP) statistics, use the **clear nmsp statistics** command.

clear nmsp statistics

Command Default

None

Command Modes

User EXEC or privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

The following is sample output from the **clear nmsp statistics** command and shows how to clear all statistics about NMSP information exchanged between the controller and connected Cisco Mobility Services Engine (MSE):

```
Controller> clear nmsp statistics
```

clear wireless ccx statistics

To clear CCX statistics, use the **clear wireless ccx statistics** command.

clear wireless ccx statistics

Command Default

None

Command Modes

User EXEC or privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

The following is sample output from the **clear wireless ccx statistics** command and shows how to clear all collected statistics about CCX clients:

```
Controller> clear wireless ccx statistics
```

clear wireless client tsm dot11

To clear the traffic stream metrics (TSM) statistics for a particular access point or all the access points to which this client is associated, use the **clear wireless client tsm dot11** command.

clear wireless client tsm dot11 {**24ghz**| **5ghz**} *client-mac-addr* {**all**| **name** *ap-name*}

Syntax Description

24ghz	Specifies the 802.11a network.
5ghz	Specifies the 802.11b network.
client-mac-addr	MAC address of the client.
all	Specifies all access points.
name *ap-name*	Name of a Cisco lightweight access point.

Command Default

None

Command Modes

User EXEC or privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

The following is sample output from the **clear wireless client tsm dot11** command and shows how to clear the TSM for the MAC address 00:40:96:a8:f7:98 on all the access points 5-GHz radios where this client is known:

```
Controller> clear wireless client tsm dot11 5ghz 00:40:96:a8:f7:98 all
```

clear wireless location s69 statistics

To clear statistics about S69 exchanges with CCXv5 clients, use the **clear wireless location s69 statistics** command.

clear wireless location s69 statistics

Command Default

None

Command Modes

User EXEC or privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

S69 messages are exchanged between CCXv5 clients and the wireless infrastructure. The CCXv5 client uses S69 message to request location information, that is then returned by the wireless infrastructure through a S69 response message.

Examples

The following is sample output from the **clear wireless location s69 statistics** command and shows how to clear statistics about S69 exchanges with CCXv5 clients:

```
Controller> clear wireless location s69 statistics
```

copy

To copy a file from a source to a destination, use the **copy** command in boot loader mode.

copy *filesystem:/source-file-url filesystem:/destination-file-url*

Syntax Description

filesystem:	Alias for a flash file system. Use **flash:** for the system board flash device.
/source-file-url	Path (directory) and filename (source) to be copied.
/destination-file-url	Path (directory) and filename of the destination.

Command Default

None

Command Modes

Boot loader

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Filenames and directory names are case sensitive.

Directory names are limited to 127 characters between the slashes (/); the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.

Filenames are limited to 127 characters; the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.

If you are copying a file to a new directory, the directory must already exist.

Examples

This example show how to copy a file at the root:

```
Controller# copy flash:test1.text flash:test4.text.
File "flash:test1.text" successfully copied to "flash:test4.text"
```

You can verify that the file was copied by entering the **dir** *filesystem:* boot loader command.

Related Commands

Command	Description
delete	Deletes one or more files from the specified file system.

debug call-admission wireless all

To enable debugging of the wireless Call Admission Control (CAC) feature, use the **debug call-admission wireless all** command. To disable debugging, use the **no** form of this command.

debug call-admission wireless all [**switch** *switch*]

no debug call-admission wireless all [**switch** *switch*]

Syntax Description

switch	Configures debugging options for all wireless CAC messages associated to a particular switch.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was introduced.

Examples

The following is sample output from the **debug call-admission wireless switch** command and shows how to enable debugging options for CAC messages:

```
Controller# debug call-admission wireless switch 1 all
```

debug rfid

To configure radio-frequency identification (RFID) debug options, use the **debug rfid** command. To disable debugging, use the **no** form of this command.

debug rfid {*debug_leaf_name*|**all** |**detail** |**error**|**nmsp**|**receive**}[**filter**|**switch** *switch*]

nodebug rfid {*debug_leaf_name*|**all** |**detail** |**error**|**nmsp**|**receive**}[**filter**|**switch** *switch*]

Syntax Description

debug_leaf_name	Debug leaf name.
all	Configures debugging of all RFID.
detail	Configures debugging of RFID detail.
error	Configures debugging of RFID error messages.
nmsp	Configures debugging of RFID Network Mobility Services Protocol (NMSP) messages.
receive	Configures debugging of incoming RFID tag messages.
filter	Debug flag filter name.
switch *switch*	Configures RFID debugging for controller.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was introduced.

Examples

The following is sample output from the **debug rfid** command and shows how to enable debugging of RFID error messages:

```
Controller# debug rfid error switch 1
```

debug voice diagnostics mac-address

To enable debugging of voice diagnostics for voice clients, use the **debug voice diagnostics mac-address** command. To disable debugging, use the **no** form of this command.

debug voice diagnostics mac-address*mac-address1***verbose mac-address***mac-address2***verbose**

nodebug voice diagnostics mac-address*mac-address1***verbose mac-address***mac-address2***verbose**

Syntax Description

voice diagnostics	Configures voice debugging for voice clients.
mac-address *mac-address1* **mac-address** *mac-address2*	Specifies MAC addresses of the voice clients.
verbose	Enables verbose mode for voice diagnostics.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was introduced.

Examples

The following is sample output from the **debug voice diagnostics mac-address** command and shows how to enable debugging of voice diagnostics for voice client with MAC address of 00:1f:ca:cf:b6:60:

```
Controller# debug voice diagnostics mac-address 00:1f:ca:cf:b6:60
```

debug wps mfp

To enable WPS MFP debugging options, use the **debug wps mfp** command. To disable debugging, use the no form of this command.

debug wps mfp {**all**|**capwap**|**client** |**detail**|**mm**|**report**}[**switch***switch*]

Syntax Description

wps mfp	Configures WPS MFP debugging options.
all	Displays all WPS MFP debugging messages.
capwap	Displays MFP messages.
client	Displays client MFP messages.
detail	Displays detailed MFP CAPWAP messages.
mm	Displays MFP mobility (inter-controller) messages.
report	Displays MFP reports.
switch *switch*	Displays the WPS MFP debugging for the controller.

Command Default

None.

Command Modes

User EXEC or privileged EXEC.

Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was introduced.

Usage Guidelines

Examples

This example shows how to enable WPS MFP debugging options for client:

```
Controller# debug wps mfp client switch 1
```

delete

To delete one or more files from the specified file system, use the **delete** command in boot loader mode.

delete *filesystem:/file-url...*

Syntax Description

filesystem:	Alias for a flash file system. Use **usbflash0:** for the system board flash device.
/file-url	Path (directory) and filename to delete. Separate each filename with a space.

Command Default

None

Command Modes

Boot loader

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Filenames and directory names are case sensitive.

The controller prompts you for confirmation before deleting each file.

Examples

This example shows how to delete two files:

```
Controller# delete usbflash0:test2.text usbflash0:test5.text
Are you sure you want to delete "usbflash0:test2.text" (y/n)?y
File "usbflash0:test2.text" deleted
Are you sure you want to delete "usbflash0:test5.text" (y/n)?y
File "usbflash0:test2.text" deleted
```

You can verify that the files were deleted by entering the **dir usbflash0:** boot loader command.

Related Commands

Command	Description
copy	Copies a file from a source to a destination.

dir

To display the list of files and directories on the specified file system, use the **dir** command in boot loader mode.

dir *filesystem:/file-url*

Syntax Description

filesystem:	Alias for a flash file system. Use **flash:** for the system board flash device.
/file-url	(Optional) Path (directory) and directory name whose contents you want to display. Separate each directory name with a space.

Command Default

None

Command Modes

Boot loader

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Directory names are case sensitive.

Examples

This example shows how to display the files in flash memory:

```
Controller# dir flash:
Directory of flash:/
    3  -rwx        1839   Mar 01 2002 00:48:15  config.text
   11  -rwx        1140   Mar 01 2002 04:18:48  vlan.dat
   21  -rwx          26   Mar 01 2002 00:01:39  env_vars
    9  drwx         768   Mar 01 2002 23:11:42  html
   16  -rwx        1037   Mar 01 2002 00:01:11  config.text
   14  -rwx        1099   Mar 01 2002 01:14:05  homepage.htm
   22  -rwx          96   Mar 01 2002 00:01:39  system_env_vars
   17  drwx        192    Mar 06 2002 23:22:03  c3750e-universal-mz.122-35.SE2
15998976 bytes total (6397440 bytes free)
   17  drwx        192    Mar 06 2002 23:22:03  c3750x-universal-mz.122-53.SE2
15998976 bytes total (6397440 bytes free)
```

Table 3: dir Field Descriptions

Field	Description
2	Index number of the file.

Field	Description
-rwx	File permission, which can be any or all of the following: • d—directory • r—readable • w—writable • x—executable
1644045	Size of the file.
<date>	Last modification date.
env_vars	Filename.

Related Commands

Command	Description
mkdir	Creates one or more directories.
rmdir	Removes one or more directories.

emergency-install

To perform emergency installation on your system, use the **emergency-install** command in boot loader mode.

emergency-install *url://<url>*

Syntax Description

<url>	URL and name of the file which contains the emergency installation bundle image.

Command Default

None

Command Modes

Boot loader

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The boot flash will be erased during install operation.

Examples

This example shows how to perform the emergency install operation using the contents of an image file.

```
switch: emergency-install tftp:<url>/info
The bootflash will be erased during install operation, continue (y/n)?y
Starting emergency recovery (tftp:<url> ...
Reading full image into memory.....................done
Nova Bundle Image
--------------------------------------
Kernel Address    : 0x6042d5c8
Kernel Size       : 0x317ccc/3243212
Initramfs Address : 0x60745294
Initramfs Size    : 0xdc6774/14444404
Compression Format: .mzip

Bootable image at @ ram:0x6042d5c8
Bootable image segment 0 address range [0x81100000, 0x81b80000] is in range          \
[0x80180000, 0x90000000].
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
File "sda9:c3850-recovery.bin" uncompressed and installed, entry point: 0x811060f0
Loading Linux kernel with entry point 0x811060f0 ...
Bootloader: Done loading app on core_mask: 0xf

### Launching Linux Kernel (flags = 0x5)


Initiating Emergency Installation of bundle                                      \
tftp:<url>


Downloading bundle tftp:<url>...
```

```
Validating bundle tftp:<url>...
Installing bundle tftp:<url>...
Verifying bundle tftp:<url>...
Package cat3k_caa-base.SPA.03.02.00SE.pkg is Digitally Signed
Package cat3k_caa-drivers.SPA.03.02.00.SE.pkg is Digitally Signed
Package cat3k_caa-infra.SPA.03.02.00SE.pkg is Digitally Signed
Package cat3k_caa-iosd-universalk9.SPA.150-1.EX.pkg is Digitally Signed
Package cat3k_caa-platform.SPA.03.02.00.SE.pkg is Digitally Signed
Package cat3k_caa-wcm.SPA.10.0.100.0.pkg is Digitally Signed
Preparing flash...
Syncing device...
Emergency Install successful... Rebooting
Restarting system.\ufffd


Booting...(use DDR clock 667 MHz)Initializing and Testing RAM                          \
+++@@@@@###...++@@++@@++@@++@@++@@++@@++@@done.
Memory Test Pass!

Base ethernet MAC Address: 20:37:06:ce:25:80
Initializing Flash...

flashfs[7]: 0 files, 1 directories
flashfs[7]: 0 orphaned files, 0 orphaned directories
flashfs[7]: Total bytes: 6784000
flashfs[7]: Bytes used: 1024
flashfs[7]: Bytes available: 6782976
flashfs[7]: flashfs fsck took 1 seconds....done Initializing Flash.

The system is not configured to boot automatically.  The
following command will finish loading the operating system
software:

    boot
```

exit

To return to the previous mode or exit from the CLI EXEC mode, use the **exit** command.

exit

Command Default

None

Command Modes

Privileged EXEC or global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to exit the configuration mode:

```
Controller(config)# exit
```

flash_init

To initialize the flash file system, use the **flash_init** command in boot loader mode.

flash_init

Syntax Description

This command has no arguments or keywords.

Command Default

The flash file system is automatically initialized during normal system operation.

Command Modes

Boot loader

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

During the normal boot process, the flash file system is automatically initialized.

Use this command to manually initialize the flash file system. For example, you use this command during the recovery procedure for a lost or forgotten password.

help

To display the available commands, use the **help** command in boot loader mode.

help

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Boot loader

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You can also use the question mark (?) to display a list of available boot loader commands.

license right-to-use

To configure right-to-use access point adder licenses on the controller, use the **license right-to-use** command.

license right-to-use {**activate** | **deactivate**} **ap-count** {*count* | **slot** *slot-number* | **acceptEULA** | **evaluation**}

Syntax Description

activate	Activates permanent or evaluation ap-count licenses.
deactivate	Deactivates permanent or evaluation ap-count licenses.
ap-count *count*	Specifies the number of ap-count licenses added. You can configure the number of adder licenses from 1 to 1000.
slot *slot-number*	Specifies the slot number in the controller. The slot number is always 1 for the controller.
acceptEULA	Accepts the end-user license agreement (EULA) automatically for the added ap-count licenses. **Note** By default during activation, the EULA gets displayed. If the acceptEULA is passed, the EULA content is not displayed, and you can activate the evaluation license. This option is useful for automation and scripting.
evaluation	Specifies evaluation ap-count licenses.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to activate an ap-count evaluation license:

```
Controller# license right-to-use activate ap-count evaluation
Controller# end
```

This example shows how to activate an ap-count permanent license:

```
Controller# license right-to-use deactivate ap-count evaluation
Controller# end
```

This example shows how to add a new ap-count license:

```
Controller# license right-to-use activate ap-count 500 slot 1
Controller# end
```

location

To configure location information for an endpoint, use the **location** command in global configuration mode. To remove the location information, use the **no** form of this command.

location {**admin-tag** *string*| **algorithm**| **civic-location identifier** {**host**| *id*}| **civic-location identifier** {**host**| *id*}| **elin-location** {*string* |**identifier** *id*}|
expiry{**calibrating-client***timeout-value*|**client***timeout-value*|**rouge-aps***timeout-value*|**tags***timeout-value*}|
geo-location identifier {**host**| *id*}| **notify-threshold**{**client***db*|**rouge-aps***db*|**tags***db*| **plm**{**calibrating**| {**multiband | uniband**}| **client***burst-interval*}| **prefer**{**cdp weight***priority-value*|**lldp-med weight***priority-value*|**static config weight***priority-value*}|**rfid**{**status**
|**timeout***rfid-timeout-value*|**vendor-name***name*}|**rssi-half-life** {
calibrating-client*seconds*|**client***seconds*|**rogue-aps***seconds*|**tags***seconds*}

no location {**admin-tag** *string*| **algorithm**| **civic-location identifier** {**host**| *id*}| **civic-location identifier** {**host**| *id*}| **elin-location** {*string* |**identifier** *id*}|
expiry{**calibrating-client***timeout-value*|**client***timeout-value*|**rouge-aps***timeout-value*|**tags***timeout-value*}|
geo-location identifier {**host**| *id*}| **notify-threshold**{**client***db*|**rouge-aps***db*|**tags***db*| **plm**{**calibrating**| {**multiband | uniband**}| **client***burst-interval*}| **prefer**{**cdp weight***priority-value*|**lldp-med weight***priority-value*|**static config weight***priority-value*}|**rfid**{**status**
|**timeout***rfid-timeout-value*|**vendor-name***name*}|**rssi-half-life** {
calibrating-client*seconds*|**client***seconds*|**rogue-aps***seconds*|**tags***seconds*}

Syntax Description

admin-tag*string*	Configures administrative tag or site information. Site or location information in alphanumeric format.
algorithm	Configures the algorithm used to average RSSI and SNR values.
civic-location	Configures civic location information.
identifier	Specifies the name of the civic location, emergency, or geographical location.
host	Defines the host civic or geo-spatial location.
id	Name of the civic, emergency, or geographical location. **Note** The identifier for the civic location in the LLDP-MED controller TLV is limited to 250 bytes or less. To avoid error messages about available buffer space during controller configuration, be sure that the total length of all civic-location information specified for each civic-location identifier does not exceed 250 bytes.
elin-location	Configures emergency location information (ELIN).

expiry {calibrating-client | client | rogue-aps | tags} *timeout-value*	Configures the timeout for RSSI values for calibrating clients, clients, rouge access points, and RFID tags. The valid range for the timeout parameter for calibrating clients is 1 to 3600 seconds, and the default value is 5 seconds. The valid range for the timeout parameter for clients, rogue access points, and RFID tags is 5 to 3600 seconds, and the default value is 5 seconds
geo-location	Configures geo-spatial location information.
notify-threshold {client| rogue-aps| tags} *db*	Configures the NMSP notification threshold for RSSI measurements. The valid range for the threshold parameter is 0 to 10 dB, and the default value is 0 dB.
calibrating {multiband | uniband} | client *seconds*	Configures path loss measurement (CCX S60) request for calibrating clients and burst interval for clients. The valid range for the burst interval parameter is 0 to 3600 seconds.
prefer	Sets location information source priority.
rfid	Configures RFID tag tracking for a location.
rssi-half-life	Configures the RSSI half life for various devices.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

After entering the **location civic-location identifier** global configuration command, you enter civic location configuration mode. After entering the **location geo-location identifier** global configuration command, you enter geo location configuration mode.

The civic-location identifier must not exceed 250 bytes.

The host identifier configures the host civic or geo-spatial location. If the identifier is not a host, the identifier only defines a civic location or geo-spatial template that can be referenced on the interface.

The **host** keyword defines the device location. The civic location options available for configuration using the **identifier** and the **host** keyword are the same. You can specify the following civic location options in civic location configuration mode:

- **additional-code—**Sets an additional civic location code.
- **additional-location-information—**Sets additional civic location information.
- **branch-road-name—**Sets the branch road name.
- **building—**Sets building information.
- **city—**Sets the city name.
- **country—**Sets the two-letter ISO 3166 country code.
- **county—**Sets the county name.
- **default—**Sets a command to its defaults.
- **division—**Sets the city division name.
- **exit—**Exits from the civic location configuration mode.
- **floor—**Sets the floor number.
- **landmark—**Sets landmark information.
- **leading-street-dir—**Sets the leading street direction.
- **name—**Sets the resident name.
- **neighborhood—**Sets neighborhood information.
- **no—**Negates the specified civic location data and sets the default value.
- **number—**Sets the street number.
- **post-office-box—**Sets the post office box.
- **postal-code—**Sets the postal code.
- **postal-community-name—**Sets the postal community name.
- **primary-road-name—**Sets the primary road name.
- **road-section—**Sets the road section.
- **room—**Sets room information.
- **seat—**Sets seat information.
- **state—**Sets the state name.
- **street-group—**Sets the street group.
- **street-name-postmodifier—**Sets the street name postmodifier.
- **street-name-premodifier—**Sets the street name premodifier.
- **street-number-suffix—**Sets the street number suffix.
- **street-suffix—**Sets the street suffix.
- **sub-branch-road-name—**Sets the sub-branch road name.
- **trailing-street-suffix—**Sets the trailing street suffix.
- **type-of-place—**Sets the type of place.

- **unit—**Sets the unit.

You can specify the following geo-spatial location information in geo-location configuration mode:

- **altitude—**Sets altitude information in units of floor, meters, or feet.
- **latitude—**Sets latitude information in degrees, minutes, and seconds. The range is from -90 degrees to 90 degrees. Positive numbers indicate locations north of the equator.
- **longitude—**Sets longitude information in degrees, minutes, and seconds. The range is from -180 degrees to 180 degrees. Positive numbers indicate locations east of the prime meridian.
- **resolution—**Sets the resolution for latitude and longitude. If the resolution value is not specified, default value of 10 meters is applied to latitude and longitude resolution parameters. For latitude and longitude, the resolution unit is measured in meters. The resolution value can also be a fraction.
- **default—**Sets the geographical location to its default attribute.
- **exit—**Exits from geographical location configuration mode.
- **no—**Negates the specified geographical parameters and sets the default value.

Use the **no lldp med-tlv-select location information** interface configuration command to disable the location TLV. The location TLV is enabled by default.

Examples

This example shows how to configure civic location information on the controller:

```
Controller(config)# location civic-location identifier 1
Controller(config-civic)# number 3550
Controller(config-civic)# primary-road-name "Cisco Way"
Controller(config-civic)# city "San Jose"
Controller(config-civic)# state CA
Controller(config-civic)# building 19
Controller(config-civic)# room C6
Controller(config-civic)# county "Santa Clara"
Controller(config-civic)# country US
Controller(config-civic)# end
```

You can verify your settings by entering the **show location civic-location** privileged EXEC command.

This example shows how to configure the emergency location information on the controller:

```
Controller(config)# location elin-location 14085553881 identifier 1
```

You can verify your settings by entering the **show location elin** privileged EXEC command.

The example shows how to configure geo-spatial location information on the controller:

```
Controller(config)# location geo-location identifier host
Controller(config-geo)# latitude 12.34
Controller(config-geo)# longitude 37.23
Controller(config-geo)# altitude 5 floor
Controller(config-geo)# resolution 12.34
```

You can use the **show location geo-location identifier** command to display the configured geo-spatial location details.

location algorithm

To configure the algorithm used to average RSSI and SNR values, use the **location algorithm** command. To remove the algorithm used to average RSSI and SNR values, use the **no** form of this command.

location algorithm {**rssi-average**| **simple**}

no location algorithm {**rssi-average**| **simple**}

Syntax Description

rssi-average	Specifies a more accurate algorithm but with more CPU overhead.
simple	Specifies faster algorithm with smaller CPU overhead but less accuracy.

Command Default

RSSI average

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to configure a more accurate algorithm but with more CPU overhead:

```
Controller# configure terminal
Controller(config)# location algorithm rssi-average
Controller(config)# end
```

location expiry

To configure the timeout for RSSI values, use the **location expiry** command.

location expiry {**calibrating-client**| **client**| **rogue-aps**| **tags**}*timeout-value*

Syntax Description

calibrating-client	Specifies the RSSI timeout value for calibrating clients.
client	(Optional) Specifies the RSSI timeout value for clients.
rogue-aps	Specifies the RSSI timeout value for rogue access points.
tags	Specifies the RSSI timeout value for RFID tags.
timeout-value	The valid range for the timeout parameter for calibrating clients is 1 to 3600 seconds, and the default value is 5 seconds. The valid range for the timeout parameter for clients, rogue access points, and RFID tags is 5 to 3600 seconds, and the default value is 5 seconds.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to set the RSSI timeout value for wireless clients:

```
Controller# configure terminal
Controller(config)# location expiry client 1000
Controller(config)# end
```

location notify-threshold

To configure the NMSP notification threshold for RSSI measurements, use the **location notify-threshold** command. To remove the NMSP notification threshold for RSSI measurements, use the **no** form of this command.

location notify-threshold {**client**| **rogue-aps**| **tags**} *db*

no location notify-threshold {**client**| **rogue-aps**| **tags**}

Syntax Description

client	Specifies the NMSP notification threshold (in dB) for clients and rogue clients. The valid range for the threshold parameter is 0 to 10 dB, and the default value is 0 dB.
rogue-aps	Specifies the NMSP notification threshold (in dB) for rogue access points. The valid range for the threshold parameter is 0 to 10 dB, and the default value is 0 dB.
tags	Specifies the NMSP notification threshold (in dB) for RFID tags. The valid range for the threshold parameter is 0 to 10 dB, and the default value is 0 dB.
db	The valid range for the threshold parameter is 0 to 10 dB, and the default value is 0 dB.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to configure the NMSP notification threshold to 10 dB for clients. A notification NMSP message is sent to MSE as soon as the client RSSI changes by 10 dB:

```
Controller# configure terminal
Controller(config)# location notify-threshold client 10
Controller(config)# end
```

location plm calibrating

To configure path loss measurement (CCX S60) request for calibrating clients, use the **location plm calibrating** command.

location plm calibrating {**multiband**| **uniband**}

Syntax Description

multiband	Specifies the path loss measurement request for calibrating clients on the associated 802.11a or 802.11b/g radio.
uniband	Specifies the path loss measurement request for calibrating clients on the associated 802.11a/b/g radio.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The uniband is useful for a single radio clients (even if the radio is a dual band and can operate in the 2.4-GHz and the 5-GHz bands). The multiband is useful for multiple radio clients.

Examples

This example shows how to configure the path loss measurement request for calibrating clients on the associated 802.11a/b/g radio:

```
Controller# configure terminal
Controller(config)# location plm calibrating uniband
Controller(config)# end
```

location rfid

To configure RFID tag tracking for a location, use the **location rfid** command. To remove a RFID tag tracking for a location, use the **no** form of this command.

location rfid {**status**| **timeout** *seconds*| **vendor-name** *name*}

no location rfid {**status**| **timeout** *seconds*| **vendor-name**}

Syntax Description

status	Enables location tracking for RFID tags. The **no location rfid status** command disables location tracking for tags.
timeout *seconds*	Specifies the location RFID timeout value. Determines the amount of time for which a detected RFID location information is considered as valid. Any RSSI change (below the RSSI threshold) in the configured interval do not result in a new location computation and a message is sent to the MSE. The valid timeout range is from 60 through 7200 seconds.
vendor-name *name*	Specifies the RFID tag vendor name.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The **no location rfid status** command disables location RFID status. The **no location rfid timeout** command returns to the default timeout value. The **no location rfid vendor-name** disables tracking for a particular vendor.

Examples

The example shows how to configure the static RFID tag data timeout:

```
Controller# configure terminal
Controller(config)# location rfid timeout 1000
Controller(config)# end
```

location rssi-half-life

To configure the RSSI half life for various devices, use the **location rssi-half-life** command. To remove a RSSI half life for various devices, use the **no** form of this command.

location rssi-half-life {**calibrating-client**| **client**| **rogue-aps**| **tags**} *seconds*

no location rssi-half-life {**calibrating-client**| **client**| **rogue-aps**| **tags**}

Syntax Description

calibrating-client	Specifies the RSSI half life for calibrating clients.
client	Specifies the RSSI half life for clients.
rogue-aps	Specifies the RSSI half life for rogue access points.
tags	Specifies the RSSI half life for RFID tags.
seconds	The valid range for the half-life parameter is 0, 1, 2, 5, 10, 20, 30, 60, 90, 120, 180, or 300 seconds, and the default value is 0 seconds.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to configure the half life value for a client RSSI to be 100 seconds:

```
Controller# configure terminal
Controller(config)# location rssi-half-life client 100
Controller(config)# end
```

mac address-table move update

To enable the MAC address-table move update feature, use the **mac address-table move update** command in global configuration mode on thecontroller stack or on a standalone controller. To return to the default setting, use the **no** form of this command.

mac address-table move update {**receive** | **transmit**}

no mac address-table move update {**receive** | **transmit**}

Syntax Description

receive	Specify that the controller processes MAC address-table move update messages.
transmit	Specify that the controller sends MAC address-table move update messages to other controlleres in the network if the primary link goes down and the standby link comes up.

Command Default

By default, the MAC address-table move update feature is disabled.

Command Modes

Global configuration.

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The MAC address-table move update feature allows the controller to provide rapid bidirectional convergence if a primary (forwarding) link goes down and the standby link begins forwarding traffic.

You can configure the accesscontroller to send the MAC address-table move update messages if the primary link goes down and the standby link comes up. You can configure the uplinkcontrolleres to receive and process the MAC address-table move update messages.

Examples

This example shows how to configure an access controller to send MAC address-table move update messages:

```
Controller# configure terminal
Controller# mac address-table move update transmit
Controller# end
```

This example shows how to configure an uplink controller to get and process MAC address-table move update messages:

```
Controller# configure terminal
Controller# mac address-table move update receive
```

```
Controller# end
```

You can verify your settings by entering the **show mac address-table move update** privileged EXEC command.

Related Commands

Command	Description
clear mac address-table move update	Clears the MAC address-table move update global counters.
debug matm move update	Debugs the MAC address-table move update message processing.
show mac address-table move update	Displays the MAC address-table move update information on the controller.

mgmt_init

To initialize the Ethernet management port, use the **mgmt_init**command in boot loader mode.

mgmt_init

Command Default

None

Command Modes

Boot loader

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Use the **mgmt_init** command only during debugging of the Ethernet management port.

Examples

This example shows how to initialize the Ethernet management port:

```
Controller# mgmt_init
```

mkdir

To create one or more directories on the specified file system, use the **mkdir** command in boot loader mode.

mkdir *filesystem:/directory-url...*

Syntax Description

filesystem:	Alias for a flash file system. Use **usbflash0:** for the system board flash device.
/directory-url	Name of the directories to create. Separate each directory name with a space.

Command Default

None

Command Modes

Boot loader

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Directory names are case sensitive.

Directory names are limited to 127 characters between the slashes (/); the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.

Examples

This example shows how to make a directory called Saved_Configs:

```
Controller# mkdir usbflash0:Saved_Configs
Directory "usbflash0:Saved_Configs" created
```

This example shows how to make two directories:

```
Controller# mkdir usbflash0:Saved_Configs1 flash:Test
Directory "usbflash0:Saved_Configs1" created
Directory "usbflash0:Test" created
```

You can verify that the directory was created by entering the **dir** *filesystem:* command in boot loader mode.

Related Commands

Command	Description
dir	Displays a list of files and directories on the specified file system.

Command	Description
rmdir	Removes one or more directories from the specified file system.

more

To display the contents of one or more files, use the **more** command in boot loader mode.

more *filesystem:/file-url...*

Syntax Description

filesystem:	Alias for a flash file system. Use **flash:** for the system board flash device.
/file-url	Path (directory) and name of the files to display. Separate each filename with a space.

Command Default

None

Command Modes

Boot loader

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Filenames and directory names are case sensitive.

If you specify a list of files, the contents of each file appears sequentially.

Examples

This example shows how to display the contents of a file.

```
Controller# more flash:image_file_name/info
version_suffix: universal-122-xx.SEx
version_directory: image_file_name
image_system_type_id: 0x00000002
image_name: image_file_name.bin
ios_image_file_size: 8919552
total_image_file_size: 11592192
image_feature: IP|LAYER_3|PLUS|MIN_DRAM_MEG=128
image_family: family
stacking_number: 1.34
board_ids: 0x00000068 0x00000069 0x0000006a 0x0000006b
info_end:
```

Related Commands

Command	Description
cat	Displays the contents of one or more files.

Command	Description
type	Displays the contents of one or more files.

nmsp notification interval

To modify the Network Mobility Services Protocol (NMSP) notification interval value on the controller to address latency in the network, use the **nmsp notification interval** command.

nmsp notification interval {**attachment**| **location**| **rssi** {**clients**| **rfid**| **rogues** {**ap**| **client**}}} *interval*

Syntax Description

attachment	Specifies the time used to aggregate attachment information.
location	Specifies the time used to aggregate location information.
rssi	Sets the RSSI measurement interval.
clients	Modifies the interval for clients.
rfid	Modifies the interval for active radio frequency identification (RFID) tags.
rogues	Modifies the interval for rogue access points and rogue clients.
ap	Specifies measurement interval for rogue APs.
client	Specifies measurement interval for rogue clients.
interval	Time interval. The range is from 1 to 30 seconds. The default time interval is 2 seconds for clients, RFID tags, and rogue APs and clients. The default time interval is 30 seconds for attachment and location.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to modify the NMSP notification interval for the active RFID tags to 25 seconds:

```
Controller# configure terminal
Controller(config)# nmsp notification-interval measurement rfid 25
Controller(config)# end
```

This example shows how to modify NMSP notification intervals about devices attachment (connecting to the network or disconnecting from the network) every 10 seconds:

```
Controller# configure terminal
Controller(config)# nmsp notification-interval attachment 10
Controller(config)# end
```

This example shows how to configure NMSP notification intervals about location parameters (location change) every 20 seconds:

```
Controller# configure terminal
Controller(config)# nmsp notification-interval location 20
Controller(config)# end
```

rename

To rename a file, use the **rename** command in boot loader mode.

rename *filesystem:/source-file-url filesystem:/destination-file-url*

Syntax Description

filesystem:	Alias for a flash file system. Use **usbflash0:** for the system board flash device.
/source-file-url	Original path (directory) and filename.
/destination-file-url	New path (directory) and filename.

Command Default

None

Command Modes

Boot loader

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Filenames and directory names are case sensitive.

Directory names are limited to 127 characters between the slashes (/); the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.

Filenames are limited to 127 characters; the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.

Examples

This example shows a file named *config.text* being renamed to *config1.text*:

```
Controller# rename usbflash0:config.text usbflash0:config1.text
```

You can verify that the file was renamed by entering the **dir** *filesystem :* boot loader command.

Related Commands

Command	Description
copy	Copies a file from a source to a destination.

reset

To perform a hard reset on the system, use the **reset** command in boot loader mode. A hard reset is similar to power-cycling the controller; it clears the processor, registers, and memory.

reset

Command Default

None

Command Modes

Boot loader

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to reset the system:

```
Controller# reset
Are you sure you want to reset the system (y/n)?y
System resetting...
```

Related Commands

Command	Description
boot	Loads and boots an executable image and enters the command-line interface.

rmdir

To remove one or more empty directories from the specified file system, use the **rmdir** command in boot loader mode.

rmdir *filesystem:/directory-url...*

Syntax Description

filesystem:	Alias for a flash file system. Use **usbflash0:** for the system board flash device.
/directory-url	Path (directory) and name of the empty directories to remove. Separate each directory name with a space.

Command Default

None

Command Modes

Boot loader

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Directory names are case sensitive and limited to 45 characters between the slashes (/); the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.

Before removing a directory, you must first delete all the files in the directory.

The controller prompts you for confirmation before deleting each directory.

Examples

This example shows how to remove a directory:

```
Controller# rmdir usbflash0:Test
```

You can verify that the directory was deleted by entering the **dir** *filesystem:* boot loader command.

Related Commands

Command	Description
dir	Displays a list of files and directories on the specified file system.
mkdir	Creates one or more new directories on the specified file system.

set

To set or display environment variables, use the **set** command in boot loader mode. Environment variables can be used to control the boot loader or any other software running on the controller.

set *variable value*

Syntax Description

variable value	Use one of these keywords for *variable* and *value*: **MANUAL_BOOT—**Decides whether the controller automatically or manually boots. Valid values are 1, yes, 0, and no. If it is set to no or 0, the boot loader attempts to automatically boot the system. If it is set to anything else, you must manually boot the controller from the boot loader mode.
	BOOT *filesystem:/file-url***—**A semicolon-separated list of executable files to try to load and execute when automatically booting. If the BOOT environment variable is not set, the system attempts to load and execute the first executable image it can find by using a recursive, depth-first search through the flash: file system. If the BOOT variable is set but the specified images cannot be loaded, the system attempts to boot the first bootable file that it can find in the flash file system.
	ENABLE_BREAK—Decides whether the automatic boot process can be interrupted by using the Break key on the console. Valid values are 1, yes, on, 0, no, and off. If it is set to 1, yes, or on, you can interrupt the automatic boot process by pressing the Break key on the console after the flash file system has initialized.
	HELPER *filesystem:/file-url***—**A semicolon-separated list of loadable files to dynamically load during the boot loader initialization. Helper files extend or patch the functionality of the boot loader.
	PS1 *prompt***—**A string that is used as the command-line prompt in boot loader mode.
	CONFIG_FILE flash: */file-url***—**The filename that Cisco IOS uses to read and write a nonvolatile copy of the system configuration.
	BAUD *rate***—**The rate in bits per second (b/s) used for the console. The Cisco IOS software inherits the baud rate setting from the boot loader and continues to use this value unless the configuration file specifies another setting. The range is from 0 to 4294967295 b/s. Valid values are 50, 75, 110, 150, 300, 600, 1200, 1800, 2000, 2400, 3600, 4800, 7200, 9600, 14400, 19200, 28800, 38400, 56000, 57600, 115200, and 128000. The most commonly used values are 300, 1200, 2400, 9600, 19200, 57600, and 115200.

Command Default

The environment variables have these default values:

MANUAL_BOOT: No (0)

BOOT: Null string

ENABLE_BREAK: No (Off or 0) (the automatic boot process cannot be interrupted by pressing the Break key on the console).

HELPER: No default value (helper files are not automatically loaded).

PS1: controller:

CONFIG_FILE: config.text

BAUD: 9600 b/s

SWITCH_NUMBER: 1

SWITCH_PRIORITY: 1

Note Environment variables that have values are stored in the flash file system in various files. The format of these files is that each line contains an environment variable name and an equal sign followed by the value of the variable. A variable has no value if it is not listed in this file; it has a value if it is listed in the file even if the value is a null string. A variable that is set to a null string (for example, " ") is a variable with a value. Many environment variables are predefined and have default values.

Command Modes

Boot loader

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Environment variables are case sensitive and must be entered as documented.

Environment variables that have values are stored in flash memory outside of the flash file system.

Under normal circumstances, it is not necessary to alter the setting of the environment variables.

The MANUAL_BOOT environment variable can also be set by using the **boot manual** global configuration command.

The BOOT environment variable can also be set by using the **boot system** *filesystem:/file-url* global configuration command.

The ENABLE_BREAK environment variable can also be set by using the **boot enable-break** global configuration command.

The HELPER environment variable can also be set by using the **boot helper** *filesystem: / file-url* global configuration command.

The CONFIG_FILE environment variable can also be set by using the **boot config-file flash:** */file-url* global configuration command.

The SWITCH_NUMBER environment variable can also be set by using the **switch** *current-stack-member-number* **renumber** *new-stack-member-number* global configuration command.

The SWITCH_PRIORITY environment variable can also be set by using the controller *stack-member-number* **priority** *priority-number* global configuration command.

The boot loader prompt string (PS1) can be up to 120 printable characters except the equal sign (=).

Examples

This example shows how to change the boot loader prompt:

```
Controller# set PS1 loader:
loader:
```

You can verify your setting by using the **set** boot loader command.

Related Commands

Command	Description
unset	Resets one or more environment variables to its previous setting.

show cable-diagnostics tdr

To display the Time Domain Reflector (TDR) results, use the **show cable-diagnostics tdr** command in privileged EXEC mode.

show cable-diagnostics tdr interface *interface-id*

Syntax Description

interface-id	Specifies the interface on which TDR was run.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

TDR is supported only on 10/100/100 copper Ethernet ports. It is not supported on 10-Gigabit Ethernet ports and small form-factor pluggable (SFP) module ports.

Examples

This is an example of output from the **show cable-diagnostics tdr interface** *interface-id* command on a controller:

```
Controller# show cable-diagnostics tdr interface gigabitethernet1/0/23
TDR test last run on: March 01 00:04:08
Interface  Speed  Local pair  Pair length         Remote pair   Pair status
---------  -----  ----------  -----------------  -----------  --------------------
Gi1/0/23   1000M  Pair A      1    +/- 1 meters   Pair A        Normal
                  Pair B      1    +/- 1 meters   Pair B        Normal
                  Pair C      1    +/- 1 meters   Pair C        Normal
                  Pair D      1    +/- 1 meters   Pair D        Normal
```

Table 4: Fields Descriptions for the show cable-diagnostics tdr Command Output

Field	Description
Interface	Interface on which TDR was run.
Speed	Speed of connection.

Field	Description
Local pair	Name of the pair of wires that TDR is testing on the local interface.
Pair length	Location on the cable where the problem is, with respect to your controller. TDR can only find the location in one of these cases: • The cable is properly connected, the link is up, and the interface speed is 1000 Mb/s. • The cable is open. • The cable has a short.
Remote pair	Name of the pair of wires to which the local pair is connected. TDR can learn about the remote pair only when the cable is properly connected and the link is up.
Pair status	The status of the pair of wires on which TDR is running: • Normal—The pair of wires is properly connected. • Not completed—The test is running and is not completed. • Not supported—The interface does not support TDR. • Open—The pair of wires is open. • Shorted—The pair of wires is shorted. • ImpedanceMis—The impedance is mismatched. • Short/Impedance Mismatched—The impedance mismatched or the cable is short. • InProgress—The diagnostic test is in progress

This is an example of output from the **show interface** *interface-id* command when TDR is running:

```
Controller# show interface gigabitethernet1/0/2
gigabitethernet1/0/2 is up, line protocol is up (connected: TDR in Progress)
```

This is an example of output from the **show cable-diagnostics tdr interface** *interface-id* command when TDR is not running:

```
Controller# show cable-diagnostics tdr interface gigabitethernet1/0/2
% TDR test was never issued on Gi1/0/2
```

If an interface does not support TDR, this message appears:

```
% TDR test is not supported on controller 1
```

Related Commands

Command	Description
test cable-diagnostics tdr	Enables and runs TDR on an interface.

show license right-to-use

To display the detailed information of ap-count adder licenses installed on the controller, use the **show license right-to-use** command.

show licenseright-to-use{**detail | eula | usage | summary**}

Syntax Description

detail	Displays details of all the licenses.
eula	Displays the EULA content for the adder and evaluation ap-count licenses.
usage	Displays the usage details of all licenses.
summary	Displays the summary of licenses that are currently in use.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

The following is sample output from the **show license right-to-use** command and displays all the available licenses:

```
Controller#  show license right-to-use
 Slot#  License name   Type     Count   Period left
-------------------------------------------------------
 1      apcount      evaluation    1000  Expired
 1      apcount      adder         125   Lifetime
```

The following is sample output from the **show license right-to-use usage** command and displays the usage of licenses:

```
Controller#  show license right-to-use usage
 Slot#  License Name     Type     usage-duration(y:m:d)  In-Use  EULA
-------------------------------------------------------------------------
 1      apcount        evaluation    0 :2 :14            no        no
 1      apcount        adder         0 :0 :1             yes       yes
```

The following is sample output from the **show license right-to-use detail** command and displays the detailed information of licenses:

```
Controller#  show license right-to-use detail

Index 1:  License Name: apcount
           Period left: 16
           License Type: evaluation
           License State: Not Activated
           License Count: 1000
           License Location: Slot 1
Index 2:  License Name: apcount
           Period left: Lifetime
           License Type: adder
           License State: Active, In use
           License Count: 125
           License Location: Slot 1
```

The following is sample output from the **show license right-to-use summary** command when the evaluation license is active:

```
Controller#  show license right-to-use summary
  License Name    Type     Count   Period left
------------------------------------------------
  apcount      evaluation  1000     50

----------------------------------------------

Evaluation AP-Count: Enabled
Total AP Count Licenses: 1000
AP Count Licenses In-use: 100
AP Count Licenses Remaining: 900
```

The following is sample output from the **show license right-to-use summary** command when the adder licenses are active:

```
Controller#
  License Name    Type     Count   Period left
------------------------------------------------
apcount      adder       125      Lifetime

----------------------------------------------

Evaluation AP-Count: Disabled
Total AP Count Licenses: 125
AP Count Licenses In-use: 100
AP Count Licenses Remaining: 25
```

show location

To display location information, use the **show location** command.

show location {**detail** *mac-addr*| **plm**| **statistics**| **summary rfid**| **rfid** {**client**| **config**| **detail** *MAC-addr*| **summary**}}

Syntax Description

detail *mac-addr*	Displays detailed location information with the RSSI table for a particular client.
plm	Displays location path loss measurement (CCX S60) configuration.
statistics	Displays location-based system statistics.
summary	Displays location-based system summary information.
rfid	Displays the RFID tag tracking information.
client	Displays the summary of RFID tags that are clients.
config	Displays the configuration options for RFID tag tracking.
detail *MAC-addr*	Displays the detailed information for one rfid tag.
summary	Displays summary information for all known rfid tags.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

The following is sample output from the **show location plm** command:

```
Controller# show location plm
Location Path Loss Configuration

Calbration client      : Disabled, Radio: Multiband
Normal clients         : Disabled
Burst interval         : 60
```

show location ap-detect

To display the location information detected by specified access point, use the **show location ap-detect** command.

show location ap-detect {**all| client| rfid| rogue-ap| rogue-client**} *ap-name*

Syntax Description

all	Displays information of the client, RFID, rogue access point, and rogue client.
client	Displays the client information.
rfid	Displays RFID information.
rogue-ap	Displays rogue access point information.
rogue-client	Displays rogue client information.
ap-name	Specified access point name.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

The following is sample output from the **show location ap-detect client** command:

```
Controller# show location ap-detect client AP02
Clients

MAC Address       Status            Slot  Antenna     RSSI
------------------------------------------------------------
2477.0389.96ac    Associated           1        0      -60
2477.0389.96ac    Associated           1        1      -61
2477.0389.96ac    Associated           0        0      -46
2477.0389.96ac    Associated           0        1      -41


RFID Tags


Rogue AP's
```

```
Rogue Clients

MAC Address         State               Slot     Rssi
------------------------------------------------------
0040.96b3.bce6      Alert               1        -58
586d.8ff0.891a      Alert               1        -72
```

show mac address-table move update

To display the MAC address-table move update information on the controller, use the **show mac address-table move update** command in EXEC mode.

show mac address-table move update

Command Default

None

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This is an example of output from the **show mac address-table move update** command:

```
Controller# show mac address-table move update

Switch-ID : 010b.4630.1780
Dst mac-address : 0180.c200.0010
Vlans/Macs supported : 1023/8320
Default/Current settings: Rcv Off/On, Xmt Off/On
Max packets per min : Rcv 40, Xmt 60
Rcv packet count : 10
Rcv conforming packet count : 5
Rcv invalid packet count : 0
Rcv packet count this min : 0
Rcv threshold exceed count : 0
Rcv last sequence# this min : 0
Rcv last interface : Po2
Rcv last src-mac-address : 0003.fd6a.8701
Rcv last switch-ID : 0303.fd63.7600
Xmt packet count : 0
Xmt packet count this min : 0
Xmt threshold exceed count : 0
Xmt pak buf unavail cnt : 0
Xmt last interface : None
```

Related Commands

Command	Description
clear mac address-table move update	Clears the MAC address-table move update counters.
mac address-table move update {**receive** | **transmit**}	Configures MAC address-table move update on the controller.

show nmsp

To display the Network Mobility Services Protocol (NMSP) configuration settings, use the **show nmsp** command.

show nmsp {**attachment**| **capability**| **notification interval**| **statistics** {**connection**| **summary**}| **status**| **subscription detail [ip-addr]**| **summary**}

Syntax Description

attachment suppress interfaces	Displays attachment suppress interfaces.
capability	Displays NMSP capabilities.
notification interval	Displays the NMSP notification interval.
statistics connection	Displays all connection-specific counters.
statistics summary	Displays the NMSP counters.
status	Displays status of active NMSP connections.
subscription detail *ip-addr*	Details only for the NMSP services subscribed to by a specific IP address.
subscription summary	Displays details for all of the NMSP services to which the controller is subscribed. Details only for the NMSP services subscribed to by a specific IP address.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Examples

The following is sample output from the **show nmsp notification interval** command:

```
Controller#  show nmsp notification interval
NMSP Notification Intervals
---------------------------

RSSI Interval:
 Client               : 2 sec
 RFID                 : 2 sec
 Rogue AP             : 2 sec
 Rogue Client         : 2 sec
Attachment Interval   : 30 sec
Location Interval     : 30 sec
```

Related Commands

Command	Description
clear nmsp statistics	Clears the NMSP statistic counters.

show tech-support wireless

To display Cisco wireless LAN controller variables frequently requested by Cisco Technical Assistance Center (TAC), use the **show tech-support wireless** command.

show tech-support wireless

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

The following is sample output from the **show tech-support wireless** command:

```
Controller# show tech-support wireless
 *** show ap capwap timers ***

Cisco AP CAPWAP timers

AP Discovery timer       : 10
AP Heart Beat timeout    : 30
Primary Discovery timer  : 120
Primed Join timeout      : 0
Fast Heartbeat           : Disabled
Fast Heartbeat timeout   : 1
*** show ap capwap retransmit ***
Global control packet retransmit interval : 3
Global control packet retransmit count : 5

AP Name                          Retransmit Interval             Retransmit Count
-----------------------------------------------------------------------------------
TSIM_AP-2                        3                               5
TSIM_AP-3                        3                               5
*** show ap dot11 24ghz cleanair air-quality summary ***

AQ = Air Quality
DFS = Dynamic Frequency Selection

*** show ap dot11 24ghz cleanair air-quality worst ***

AQ = Air Quality
DFS = Dynamic Frequency Selection
AP Name             Channel   Avg AQ  Min AQ  Interferers  DFS
-------------------------------------------------------------
                    0         0       0       0            No
*** show ap dot11 24ghz cleanair config ***

Clean Air Solution................................ : Disabled
Air Quality Settings:
    Air Quality Reporting......................... : Disabled
    Air Quality Reporting Period (min)............ : 15
    Air Quality Alarms............................ : Enabled
    Air Quality Alarm Threshold................... : 10
Interference Device Settings:
```

```
    Interference Device Reporting..... : Enabled
        Bluetooth Link..... : Enabled
        Microwave Oven..... : Enabled
        802.11 FH..... : Enabled
        Bluetooth Discovery..... : Enabled
        TDD Transmitter..... : Enabled
        Jammer..... : Enabled
        Continuous Transmitter..... : Enabled
        DECT-like Phone..... : Enabled
        Video Camera..... : Enabled
        802.15.4..... : Enabled
        WiFi Inverted..... : Enabled
        WiFi Invalid Channel..... : Enabled
        SuperAG..... : Enabled
        Canopy..... : Enabled
        Microsoft Device..... : Enabled
        WiMax Mobile..... : Enabled
        WiMax Fixed..... : Enabled
    Interference Device Types Triggering Alarms:
        Bluetooth Link..... : Disabled
        Microwave Oven..... : Disabled
        802.11 FH..... : Disabled
        Bluetooth Discovery..... : Disabled
        TDD Transmitter..... : Disabled
        Jammer..... : Disabled
        Continuous Transmitter..... : Disabled
        DECT-like Phone..... : Disabled
        Video Camera..... : Disabled
  802.15.4..... : Disabled
        WiFi Inverted..... : Enabled
        WiFi Invalid Channel..... : Enabled
        SuperAG..... : Disabled
        Canopy..... : Disabled
        Microsoft Device..... : Disabled
        WiMax Mobile..... : Disabled
        WiMax Fixed..... : Disabled
    Interference Device Alarms..... : Enabled
Additional Clean Air Settings:
    CleanAir Event-driven RRM State..... : Disabled
    CleanAir Driven RRM Sensitivity..... : LOW
    CleanAir Persistent Devices state..... : Disabled
```

show wireless band-select

To display the status of the band-select configuration, use the **show wireless band-select** command.

show wireless band-select

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

The following is sample output from the **show wireless band-select** command:

```
Controller# show wireless band-select
Band Select Probe Response    : per WLAN enabling
Cycle Count                   : 2
Cycle Threshold (millisec)    : 200
Age Out Suppression (sec)     : 20
Age Out Dual Band (sec)       : 60
Client RSSI (dBm)             : 80
```

show wireless client calls

To display the total number of active or rejected calls on the controller, use the **show wireless client calls** command.

show wireless client calls {**active** | **rejected**}

Syntax Description

active	Displays active calls.
rejected	Displays rejected calls.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

The following is sample output from the **show wireless client calls** command:

```
Controller# show wireless client calls active

TSPEC Calls:

------------------------------------------------------------------------------
MAC Address     AP Name             Status               WLAN  Authenticated
------------------------------------------------------------------------------
0000.1515.000f    AP-2           Associated             1  Yes

SIP Calls:
------------------
Number of Active TSPEC calls on 802.11a and 802.11b/g: 1
Number of Active SIP calls on 802.11a and 802.11b/g: 0
```

show wireless client dot11

To display the total number of active or rejected calls for a specific band (2.4 Ghz or 5 Ghz), use the **show wireless client dot11** command.

show wireless client dot11 {**24ghz** | **5ghz**} **calls** {**active** | **rejected**}

Syntax Description

24ghz	Displays the 802.11b/g network.
5ghz	Displays the 802.11a network.
calls	Displays the wireless client calls.
active	Displays active calls
rejected	Displays rejected calls

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

The following is sample output from the **show wireless client dot11** command:

```
Controller# show wireless client dot11 5ghz calls active

 TSPEC Calls:
------------------


SIP Calls:
------------------
Number of Active TSPEC calls on 802.11a: 0
Number of Active SIP calls on 802.11a: 0
```

show wireless client location-calibration

To display the list of clients currently used to perform location calibration, use the **show wireless client location-calibration** command.

show wireless client location-calibration

Command Default None

Command Modes Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples The following is sample output from the **show wireless client location-calibration** command:

```
Controller# show wireless client location-calibration
```

show wireless client probing

To display the number of probing clients, use the **show wireless client probing** command.

show wireless client probing

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

The following is sample output from the **show wireless client probing** command:

```
Controller# show wireless client probing
MAC Address
------------------
000b.cd15.0001
000b.cd15.0002
000b.cd15.0003
000b.cd15.0004
000b.cd15.0005
000b.cd15.0006
```

show wireless client summary

To display a summary of active clients associated with the controller, use the **show wireless client summary** command.

show wireless client summary

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The following is sample output from the **show wireless client summary** command:

Use the **show wireless exclusionlist** command to display clients on the exclusion list (blacklisted).

Examples

```
Controller# show wireless client summary
Number of Local Clients : 1

MAC Address    AP Name                          WLAN State              Protocol
-------------------------------------------------------------------------------
0000.1515.000f  AP-2                        1    UP                 11a
```

show wireless client timers

To display 802.11 system timers, use the **show wireless client timers** command.

show wireless client timers

Command Default None

Command Modes Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples The following is sample output from the **show wireless client timers** command:

```
Controller# show wireless client timers
 Authentication Response Timeout (seconds)      : 10
```

show wireless client voice diagnostics

To display wireless client voice diagnostic parameters, use the **show wireless client voice diagnostics** command.

show wireless client voice diagnostics {**qos-map** | **roam-history** | **rssi** | **status** | **tspec**}

Syntax Description

qos-map	Displays information about the QoS and DSCP mapping and packet statistics in each of the four queues: VO, VI, BE, BK. The different DSCP values are also displayed.
roam-history	Displays information about the last 3 roaming histories for each known client. The output contains the timestamp, access point associated with roaming, roaming reason, and if there is a roaming failure, a reason for the roaming-failure.
rssi	Displays the client's RSSI values in the last 5 seconds when voice diagnostics are enabled.
status	Displays status of voice diagnostics for clients.
tspec	Displays if voice diagnostics are enabled for TSPEC clients.

Command Default

None

Command Modes

Privileged EXEC

Usage Guidelines

Debug voice diagnostics must be enabled for voice diagnostics to work.

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

The following is sample output from the **show wireless client voice diagnostics status** command:

```
Controller# show wireless client voice diagnostics status
Voice Diagnostics Status: FALSE
```

show wireless country

To display the configured country and the radio types supported, use the **show wireless country** command.

show wireless country {**channels**| **configured**| **supported [tx-power]**}

Syntax Description

channels	Displays the list of possible channels for each band, and the list of channels allowed in the configured countries.
configured	Display configured countries.
supported tx-power	Displays the list of allowed Tx powers in each supported country.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

The following is sample output from the **show wireless country channels** command:

```
Controller# show wireless country channels
  Configured Country...........................: US  - United States
      KEY: * = Channel is legal in this country and may be configured manually.
           A = Channel is the Auto-RF default in this country.
           . = Channel is not legal in this country.
           C = Channel has been configured for use by Auto-RF.
           x = Channel is available to be configured for use by Auto-RF.
         (-,-) = (indoor, outdoor) regulatory domain allowed by this country.
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-
    802.11bg     :
    Channels     :                  1 1 1 1 1
                 : 1 2 3 4 5 6 7 8 9 0 1 2 3 4
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-
 (-A   ,-AB  )  US   :  A * * * * A * * * * A . . .
 Auto-RF         : . . . . . . . . . . . . . .
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
 802.11a         :                        1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
 Channels        : 3 3 3 4 4 4 4 4 5 5 6 6 0 0 0 1 1 2 2 2 3 3 4 4 5 5 6 6
                 : 4 6 8 0 2 4 6 8 2 6 0 4 0 4 8 2 6 0 4 8 2 6 0 9 3 7 1 5
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
 (-A   ,-AB  )  US   :  . A . A . A . A A A A A * * * * * . . . * * * A A A A *
 Auto-RF         : . . . . . . . . . . . . . . . . . . . . . . . . . . . .
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
 4.9GHz 802.11a  :
   Channels      :                  1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2
                 : 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
```

```
 US (-A   ,-AB  ): * * * * * * * * * * * * * * * * * * * * A * * * * * A
 Auto-RF         : . . . . . . . . . . . . . . . . . . . . . . . . . . . .
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
```

The following is sample output from the **show wireless country configured** command:

```
Controller# show wireless country configured
 Configured Country.............................: US  - United States
 Configured Country Codes
       US  - United States : 802.11a Indoor,Outdoor/ 802.11b / 802.11g
```

The following is sample output from the **show wireless country supported tx-power** command:

```
Controller# show wireless country supported tx-power
      KEY: ##    = Tx Power in dBm.
           ##*   = Channel supports radar detection .
           .     = Channel is not legal in this country.
           (-)   = Regulatory Domains allowed by this country.
           (-,-) = (indoor, outdoor) regulatory Domains allowed by this country.
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
    802.11bg     :
    Channels     :                       1 1 1 1 1
                 : 1 2 3 4 5 6 7 8 9 0 1 2 3 4
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 (-CE  ,-CE  )  AE  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-E   ,-E   )  AL  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-A   ,-AR  )  AR  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
 (-E   ,-E   )  AT  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-A   ,-NA  )  AU  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
 (-E   ,-    )  BA  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-E   ,-E   )  BE  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-E   ,-E   )  BG  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-E   ,-    )  BH  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-A   ,-A   )  BO  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
 (-A   ,-AR  )  BR  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
 (-E   ,-    )  BY  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-A   ,-ABN )  CA  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
 (-A   ,-ABN )  CA2 :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
 (-E   ,-E   )  CH  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-AER ,-AR  )  CL  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-E   ,-E   )  CM  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-CE  ,-CE  )  CN  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-A   ,-AR  )  CO  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
 (-A   ,-AB  )  CR  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
 (-E   ,-E   )  CY  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-E   ,-E   )  CZ  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-E   ,-E   )  DE  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-E   ,-E   )  DK  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-A   ,-ABN )  DO  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
 (-E   ,-    )  DZ  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-A   ,-AB  )  EC  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
 (-E   ,-E   )  EE  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-E   ,-E   )  EG  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-E   ,-E   )  ES  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-E   ,-E   )  FI  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-E   ,-E   )  FR  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-E   ,-E   )  GB  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-E   ,-E   )  GI  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-E   ,-E   )  GR  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-A   ,-NA  )  HK  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
 (-E   ,-    )  HR  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-E   ,-E   )  HU  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-E   ,-ER  )  ID  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-E   ,-E   )  IE  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-EI  ,-IE  )  IL  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-I   ,-I   )  ILO :   .  .  .  . 20 20 20 20 20 20 20 20 20  .
 (-A   ,-AN  )  IN  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
 (-E   ,-E   )  IQ  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-E   ,-E   )  IS  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-E   ,-E   )  IT  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-JPU ,-JPU )  J2  :  23 23 23 23 23 23 23 23 23 23 23 23 23 23
 (-JPU ,-JPU )  J3  :  23 23 23 23 23 23 23 23 23 23 23 23 23 23
```

```
(-JPQU,-PQ  )  J4  :  23 23 23 23 23 23 23 23 23 23 23 23 23 23
(-E   ,-    )  JO  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-JPU ,-JPU )  JP  :  23 23 23 23 23 23 23 23 23 23 23 23 23 23
(-ACE ,-ACEK)  KE  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  KN  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-ACE ,-ACEK)  KR  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  KW  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  KZ  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  LB  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  LI  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,     )  LK  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  LT  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  LU  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  LV  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  MC  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  ME  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  MK  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,     )  MO  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  MT  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-A   ,-NA  )  MX  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-ACE ,-AEC )  MY  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  NL  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  NO  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-A   ,-NA  )  NZ  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-E   ,-E   )  OM  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-A   ,-AR  )  PA  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-A   ,-AR  )  PE  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-A   ,-ABN )  PH  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-A   ,-ABN )  PH2 :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-E   ,-E   )  PK  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  PL  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-A   ,-A   )  PR  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-E   ,-E   )  PT  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-A   ,-A   )  PY  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-E   ,-E   )  QA  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  RO  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  RS  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-AER ,-ER  )  RU  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-AE  ,-AE  )  SA  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  SE  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-SE  )  SG  :  20 20 20 20 20 20 20 20 20 20 20 20 20 20
(-E   ,-E   )  SI  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  SK  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-ER  )  TH  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  TN  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-EI  ,-E   )  TR  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-A   ,-ANT )  TW  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-E   ,-E   )  UA  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-A   ,-AB  )  US  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-A   ,-AB  )  US2 :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-A   ,-AB  )  USL :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-A   ,-    )  USX :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-A   ,-A   )  UY  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-A   ,-AR  )  VE  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-E   ,-E   )  VN  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  ZA  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
```

show wireless detail

To display the details of the wireless parameters configured, use the **show wireless detail** command.

show wireless detail

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The following parameters are displayed:

- The wireless user idle timeout
- The controller configured RF group name
- Fast SSID change

Examples

The following is sample output from the **show wireless detail** command:

```
Controller# show wireless detail
User Timeout               : 300
RF network                 : default
Fast SSID                  : Disabled
```

show wireless dtls connections

To display the Datagram Transport Layer Security (DTLS) server status, use the **show wireless dtls connections** command.

show wireless dtls connections

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

The following is sample output from the **show wireless dtls connections** command:

```
Controller# show wireless dtls connections
 AP Name         Local Port   Peer IP    Peer Port  Ciphersuite
------------------------------------------------------------------------
  AP-2       Capwap_Ctrl   10.0.0.16     52346      TLS_RSA_WITH_AES_128_CBC_SHA
  AP-3       Capwap_Ctrl   10.0.0.17     52347      TLS_RSA_WITH_AES_128_CBC_SHA
```

show wireless load-balancing

To display the status of the load-balancing feature, use the **show wireless load-balancing** command.

show wireless load-balancing

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

The following is sample output from the **show wireless load-balancing** command:

```
 > show wireless load-balancing
Aggressive Load Balancing.........................: per WLAN enabling
Aggressive Load Balancing Window (clients)..................:: 5
Aggressive Load Balancing Denial Count......................:: 3

Statistics
Total Denied Count (clients)................................:: 0
Total Denial Sent (messages)................................:: 0
Exceeded Denial Max Limit Count (times).....................:: 0
None 5G Candidate Count (times).............................:: 0
None 2.4G Candidate Count (times)...........................:: 0
```

show wireless performance

To display aggressive load balancing configuration, use the **show wireless performance** command.

show wireless performance {**ap**| **client**} **summary**

Syntax Description

ap summary	Displays aggressive load balancing configuration of access points configured to the controller.
client summary	Displays aggressive load balancing configuration details of the clients.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

The following is sample output from the **show wireless performance ap summary** command.

```
Controller# show wireless performance ap summary
Number of APs:
```

The following is sample output from the **show wireless performance client summary** command.

```
Controller# show wireless performance client summary
Number of Clients:

MAC Address        AP Name           Status        WLAN/Guest-Lan Auth Protocol Port Wired
-------------------------------------------------------------------------------------------
```

show wireless pmk-cache

To display information about the pairwise master key (PMK) cache, use the **show wireless pmk-cache** command.

show wireless pmk-cache[**mac-address** *mac-addr*]

Syntax Description

mac-address *mac-addr*	(Optional) Information about a single entry in the PMK cache.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

The following is sample output from the **show wireless pmk-cache mac-address** command:

```
Controller# show wireless pmk-cache mac-address H.H.H
Number of PMK caches in total : 0
```

show wireless probe

To display the advanced probe request filtering configuration and the number of probes sent to the WLAN controller per access point per client and the probe interval in milliseconds, use the **show wireless probe** command.

show wireless probe

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

The following is sample output from the **show wireless probe** command:

```
Controller# show wireless probe
Probe request filtering                          : Enabled
Number of probes per client per radio fwd from AP: 2
Probe request rate-limiting interval             : 500 msec
Aggregate probe request interval                 : 500 msec
```

show wireless sip preferred-call-no

To display SIP preferred call numbers, use the **show wireless sip preferred-call-no** command.

show wireless sip preferred-call-no

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

The following is sample output from the **show wireless sip preferred-call-no** command:

```
Controller# show wireless sip preferred-call-no
Index Preferred-Number
----------------------
1     1031
2     1032
4     1034
```

show wireless summary

To display the number of access points, radios and wireless clients known to the controller, use the **show wireless summary** command.

show wireless summary

Command Default None

Command Modes Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples The following is sample output from the **show wireless summary** command:

```
Controller# show wireless summary

Access Point Summary

               Total    Up    Down
-------------------------------------
802.11a/n          2     2       0
802.11b/g/n        2     2       0
All APs            2     2       0

Client Summary

Current Clients : 1
Excluded Clients: 0
Disabled Clients: 0
```

shutdown

To shutdown the system elements, use the **shutdown** command. To disable the configuration set, use the the **no** form of this command.

shutdown

{**no shutdown**}

Command Default None

Command Modes Privileged EXEC or global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples This example shows how to shut down a WLAN:

```
Controller(config)# wlan open1
Controller(config-wlan)# shutdown
```

This example shows not to shut down an access point:

```
Controller# configure terminal
Controller(config)# ap name 3602a no shutdown
```

system env temperature threshold yellow

To configure the difference between the yellow and red temperature thresholds that determines the value of yellow threshold, use the **system env temperature threshold yellow** command in global configuration mode. To return to the default value, use the **no** form of this command.

system env temperature threshold yellow *value*

no system env temperature threshold yellow *value*

Syntax Description

value	Specifies the difference between the yellow and red threshold values (in Celsius). The range is 10 to 25.

Command Default

These are the default values

Table 5: Default Values for the Temperature Thresholds

controller	Difference between Yellow and Red	Red[1]
Catalyst 3850	14°C	60°C

1 You cannot configure the red temperature threshold.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You cannot configure the green and red thresholds but can configure the yellow threshold. Use the **system env temperature threshold yellow** *value* global configuration command to specify the difference between the yellow and red thresholds and to configure the yellow threshold. For example, if the red threshold is 66 degrees C and you want to configure the yellow threshold as 51 degrees C, set the difference between the thresholds as 15 by using the **system env temperature threshold yellow 15** command. For example, if the red threshold is 60 degrees C and you want to configure the yellow threshold as 51 degrees C, set the difference between the thresholds as 15 by using the **system env temperature threshold yellow 9** command.

Note The internal temperature sensor in thecontroller measures the internal system temperature and might vary ±5 degrees C.

Examples

This example sets 15 as the difference between the yellow and red thresholds:

```
Controller(config)# system env temperature threshold yellow 15
Controller(config)#
```

Related Commands

Command	Description
show env temperature status	Displays the temperature status and threshold levels.

test cable-diagnostics tdr

To run the Time Domain Reflector (TDR) feature on an interface, use the **test cable-diagnostics tdr** command in privileged EXEC mode.

test cable-diagnostics tdr interface *interface-id*

Syntax Description

interface-id	Specifies the interface on which to run TDR.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

TDR is supported only on 10/100/100 copper Ethernet ports. It is not supported on 10-Gigabit Ethernet ports or small form-factor pluggable (SFP) module ports.

After you run TDR by using the **test cable-diagnostics tdr interface** *interface-id* command, use the **show cable-diagnostics tdr interface** *interface-id* privileged EXEC command to display the results.

Examples

This example shows how to run TDR on an interface:

```
Controller# test cable-diagnostics tdr interface gigabitethernet1/0/2
TDR test started on interface Gi1/0/2
A TDR test can take a few seconds to run on an interface
Use 'show cable-diagnostics tdr' to read the TDR results.
```

If you enter the **test cable-diagnostics tdr interface** *interface-id* command on an interface that has a link status of up and a speed of 10 or 100 Mb/s, these messages appear:

```
Controller# test cable-diagnostics tdr interface gigabitethernet1/0/3
TDR test on Gi1/0/9 will affect link state and traffic
TDR test started on interface Gi1/0/3
A TDR test can take a few seconds to run on an interface
Use 'show cable-diagnostics tdr' to read the TDR results.
```

Related Commands

Command	Description
show cable-diagnostics tdr	Displays the TDR results.

traceroute mac

To display the Layer 2 path taken by the packets from the specified source MAC address to the specified destination MAC address, use the **traceroute mac** command in privileged EXEC mode.

traceroute mac [**interface** *interface-id*] *source-mac-address* [**interface** *interface-id*] *destination-mac-address* [**vlan** *vlan-id*] **[detail]**

Syntax Description

interface *interface-id*	(Optional) Specifies an interface on the source or destination controller.
source-mac-address	Specifies the MAC address of the source controller in hexadecimal format.
destination-mac-address	Specifies the MAC address of the destination controller in hexadecimal format.
vlan *vlan-id*	(Optional) Specifies the VLAN on which to trace the Layer 2 path that the packets take from the source controller to the destination controller. Valid VLAN IDs are 1 to 4094.
detail	(Optional) Specifies that detailed information appears.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

For Layer 2 traceroute to function properly, Cisco Discovery Protocol (CDP) must be enabled on all the controlleres in the network. Do not disable CDP.

When the controller detects a device in the Layer 2 path that does not support Layer 2 traceroute, the controller continues to send Layer 2 trace queries and lets them time out.

The maximum number of hops identified in the path is ten.

Layer 2 traceroute supports only unicast traffic. If you specify a multicast source or destination MAC address, the physical path is not identified, and an error message appears.

The **traceroute mac** command output shows the Layer 2 path when the specified source and destination addresses belong to the same VLAN. If you specify source and destination addresses that belong to different VLANs, the Layer 2 path is not identified, and an error message appears.

If the source or destination MAC address belongs to multiple VLANs, you must specify the VLAN to which both the source and destination MAC addresses belong. If the VLAN is not specified, the path is not identified, and an error message appears.

The Layer 2 traceroute feature is not supported when multiple devices are attached to one port through hubs (for example, multiple CDP neighbors are detected on a port). When more than one CDP neighbor is detected on a port, the Layer 2 path is not identified, and an error message appears.

This feature is not supported in Token Ring VLANs.

Examples

This example shows how to display the Layer 2 path by specifying the source and destination MAC addresses:

```
Controller# traceroute mac 0000.0201.0601 0000.0201.0201
Source 0000.0201.0601 found on con6[WS-C3750E-24PD] (2.2.6.6)
con6 (2.2.6.6) :Gi0/0/1 => Gi0/0/3
con5                 (2.2.5.5        )  :    Gi0/0/3 => Gi0/0/1
con1                 (2.2.1.1        )  :    Gi0/0/1 => Gi0/0/2
con2                 (2.2.2.2        )  :    Gi0/0/2 => Gi0/0/1
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed
```

This example shows how to display the Layer 2 path by using the **detail** keyword:

```
Controller# traceroute mac 0000.0201.0601 0000.0201.0201 detail
Source 0000.0201.0601 found on con6[WS-C3750E-24PD] (2.2.6.6)
con6 / WS-C3750E-24PD / 2.2.6.6 :
        Gi0/0/2 [auto, auto] => Gi0/0/3 [auto, auto]
con5 / WS-C2950G-24-EI / 2.2.5.5 :
        Fa0/3 [auto, auto] => Gi0/1 [auto, auto]
con1 / WS-C3550-12G / 2.2.1.1 :
        Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
con2 / WS-C3550-24 / 2.2.2.2 :
        Gi0/2 [auto, auto] => Fa0/1 [auto, auto]
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed.
```

This example shows how to display the Layer 2 path by specifying the interfaces on the source and destination controlleres:

```
  Controller# traceroute mac interface fastethernet0/1 0000.0201.0601 interface
fastethernet0/3 0000.0201.0201
  Source 0000.0201.0601 found on con6[WS-C3750E-24PD] (2.2.6.6)
  con6 (2.2.6.6) :Gi0/0/1 => Gi0/0/3
  con5                 (2.2.5.5        )  :    Gi0/0/3 => Gi0/0/1
  con1                 (2.2.1.1        )  :    Gi0/0/1 => Gi0/0/2
  con2                 (2.2.2.2        )  :    Gi0/0/2 => Gi0/0/1
  Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
  Layer 2 trace completed
```

This example shows the Layer 2 path when the controller is not connected to the source controller:

```
  Controller#
            traceroute mac 0000.0201.0501 0000.0201.0201 detail
  Source not directly connected, tracing source .....
  Source 0000.0201.0501 found on con5[WS-C3750E-24TD] (2.2.5.5)
  con5 / WS-C3750E-24TD / 2.2.5.5 :
          Gi0/0/1 [auto, auto] => Gi0/0/3 [auto, auto]
  con1 / WS-C3550-12G / 2.2.1.1 :
          Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
  con2 / WS-C3550-24 / 2.2.2.2 :
          Gi0/2 [auto, auto] => Fa0/1 [auto, auto]
```

```
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed.
```

This example shows the Layer 2 path when the controller cannot find the destination port for the source MAC address:

```
Controller# traceroute mac 0000.0011.1111 0000.0201.0201
Error:Source Mac address not found.
Layer2 trace aborted.
```

This example shows the Layer 2 path when the source and destination devices are in different VLANs:

```
Controller# traceroute mac 0000.0201.0601 0000.0301.0201
Error:Source and destination macs are on different vlans.
Layer2 trace aborted.
```

This example shows the Layer 2 path when the destination MAC address is a multicast address:

```
Controller# traceroute mac 0000.0201.0601 0100.0201.0201
Invalid destination mac address
```

This example shows the Layer 2 path when source and destination controlleres belong to multiple VLANs:

```
Controller# traceroute mac 0000.0201.0601 0000.0201.0201
Error:Mac found on multiple vlans.
Layer2 trace aborted.
```

Related Commands

Command	Description
traceroute mac ip	Displays the Layer 2 path taken by the packets from the specified source IP address or hostname to the specified destination IP address or hostname.

traceroute mac ip

To display the Layer 2 path taken by the packets from the specified source IP address or hostname to the specified destination IP address or hostname, use the **traceroute mac ip** command in privileged EXEC mode.

traceroute mac ip {*source-ip-address*| *source-hostname*} {*destination-ip-address*| *destination-hostname*} **[detail]**

Syntax Description

source-ip-address	Specifies the IP address of the source controller as a 32-bit quantity in dotted-decimal format.
destination-ip-address	Specifies the IP address of the destination controller as a 32-bit quantity in dotted-decimal format.
source-hostname	Specifies the IP hostname of the source controller.
destination-hostname	Specifies the IP hostname of the destination controller.
detail	(Optional) Specifies that detailed information appears.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

For Layer 2 traceroute to function properly, Cisco Discovery Protocol (CDP) must be enabled on all the controlleres in the network. Do not disable CDP.

When the controller detects an device in the Layer 2 path that does not support Layer 2 traceroute, the controller continues to send Layer 2 trace queries and lets them time out.

The maximum number of hops identified in the path is ten.

The **traceroute mac ip** command output shows the Layer 2 path when the specified source and destination IP addresses are in the same subnet. When you specify the IP addresses, the controller uses Address Resolution Protocol (ARP) to associate the IP addresses with the corresponding MAC addresses and the VLAN IDs.

- If an ARP entry exists for the specified IP address, the controller uses the associated MAC address and identifies the physical path.

- If an ARP entry does not exist, the controller sends an ARP query and tries to resolve the IP address. The IP addresses must be in the same subnet. If the IP address is not resolved, the path is not identified, and an error message appears.

The Layer 2 traceroute feature is not supported when multiple devices are attached to one port through hubs (for example, multiple CDP neighbors are detected on a port). When more than one CDP neighbor is detected on a port, the Layer 2 path is not identified, and an error message appears.

This feature is not supported in Token Ring VLANs.

Examples

This example shows how to display the Layer 2 path by specifying the source and destination IP addresses and by using the **detail** keyword:

```
Controller# traceroute mac ip 2.2.66.66 2.2.22.22 detail
Translating IP to mac .....
2.2.66.66 => 0000.0201.0601
2.2.22.22 => 0000.0201.0201

Source 0000.0201.0601 found on con6[WS-C2950G-24-EI] (2.2.6.6)
con6 / WS-C3750E-24TD / 2.2.6.6 :
        Gi0/0/1 [auto, auto] => Gi0/0/3 [auto, auto]
con5 / WS-C2950G-24-EI / 2.2.5.5 :
        Fa0/3 [auto, auto] => Gi0/1 [auto, auto]
con1 / WS-C3550-12G / 2.2.1.1 :
        Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
con2 / WS-C3550-24 / 2.2.2.2 :
        Gi0/2 [auto, auto] => Fa0/1 [auto, auto]
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed.
```

This example shows how to display the Layer 2 path by specifying the source and destination hostnames:

```
Controller# traceroute mac ip con6 con2
Translating IP to mac .....
2.2.66.66 => 0000.0201.0601
2.2.22.22 => 0000.0201.0201

Source 0000.0201.0601 found on con6
con6 (2.2.6.6) :Gi0/0/1 => Gi0/0/3
con5                 (2.2.5.5        )  :    Gi0/0/3 => Gi0/1
con1                 (2.2.1.1        )  :    Gi0/0/1 => Gi0/2
con2                 (2.2.2.2        )  :    Gi0/0/2 => Fa0/1
Destination 0000.0201.0201 found on con2
Layer 2 trace completed
```

This example shows the Layer 2 path when ARP cannot associate the source IP address with the corresponding MAC address:

```
Controller# traceroute mac ip 2.2.66.66 2.2.77.77
Arp failed for destination 2.2.77.77.
Layer2 trace aborted.
```

Related Commands

Command	Description
traceroute mac	Displays the Layer 2 path taken by the packets from the specified source MAC address to the specified destination MAC address.

trapflags

To enable sending rogue access point detection traps, use the **trapflags** command. To disable sending rogue access point detection traps, use the **no** form of this command.

trapflags rogueap

no trapflags rogueap

Syntax Description

rogueap	Enables sending rogue access point detection traps.

Command Default

Enabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to disable the sending of rogue access point detection traps:

```
Controller# configure terminal
Controller(config)# no trapflags rogueap
Controller(config)# end
```

trapflags client

To enable the sending of client-related DOT11 traps, use the **trapflags client** command. To disable the sending of client-related DOT11 traps, use the **no** form of this command.

trapflags client [**dot11** {**assocfail**| **associate**| **authfail**| **deauthenticate**| **disassociate**}| **excluded**]

no trapflags client [**dot11** {**assocfail**| **associate**| **authfail**| **deauthenticate**| **disassociate**}| **excluded**]

Syntax Description

dot11	Client-related DOT11 traps.
assocfail	Enables the sending of Dot11 association fail traps to clients.
associate	Enables the sending of Dot11 association traps to clients.
authfail	Enables the sending of Dot11 authentication fail traps to clients.
deauthenticate	Enables the sending of Dot11 deauthentication traps to clients.
disassociate	Enables the sending of Dot11 disassociation traps to clients.
excluded	Enables the sending of excluded trap to clients.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to enable the sending of Dot11 disassociation trap to clients:

```
Controller# configure terminal
Controller(config)# trapflags client dot11 disassociate
Controller(config)# end
```

type

To display the contents of one or more files, use the **type** command in boot loader mode.

type *filesystem:/file-url...*

Syntax Description

filesystem:	Alias for a flash file system. Use **flash:** for the system board flash device.
/file-urll	Path (directory) and name of the files to display. Separate each filename with a space.

Command Default

None

Command Modes

Boot loader

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Filenames and directory names are case sensitive.

If you specify a list of files, the contents of each file appears sequentially.

Examples

This example shows how to display the contents of a file.

```
Controller# type flash:image_file_name/info
version_suffix: universal-122-xx.SEx
version_directory: image_file_name
image_system_type_id: 0x00000002
image_name: image_file_name.bin
ios_image_file_size: 8919552
total_image_file_size: 11592192
image_feature: IP|LAYER_3|PLUS|MIN_DRAM_MEG=128
image_family: family
stacking_number: 1.34
board_ids: 0x00000068 0x00000069 0x0000006a 0x0000006b
info_end:
```

Related Commands

Command	Description
cat	Displays the contents of one or more files.

Command	Description
more	Displays the contents of one or more files.

unset

To reset one or more environment variables, use the **unset** command in boot loader mode.

unset*variable...*

Syntax Description

variable	Use one of these keywords for *variable*:
	MANUAL_BOOT—Decides whether the controller automatically or manually boots.
	BOOT—Resets the list of executable files to try to load and execute when automatically booting. If the BOOT environment variable is not set, the system attempts to load and execute the first executable image it can find by using a recursive, depth-first search through the flash file system. If the BOOT variable is set but the specified images cannot be loaded, the system attempts to boot the first bootable file that it can find in the flash file system.
	ENABLE_BREAK—Decides whether the automatic boot process can be interrupted by using the Break key on the console after the flash file system has been initialized.
	HELPER—A semicolon-separated list of loadable files to dynamically load during the boot loader initialization. Helper files extend or patch the functionality of the boot loader.
	PS1—A string that is used as the command-line prompt in boot loader mode.
	CONFIG_FILE—Resets the filename that Cisco IOS uses to read and write a nonvolatile copy of the system configuration.
	BAUD—Resets the rate in bits per second (b/s) used for the console. The Cisco IOS software inherits the baud rate setting from the boot loader and continues to use this value unless the configuration file specifies another setting.

Command Default

None

Command Modes

Boot loader

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Under normal circumstances, it is not necessary to alter the setting of the environment variables.

The MANUAL_BOOT environment variable can also be reset by using the **no boot manual** global configuration command.

The BOOT environment variable can also be reset by using the **no boot system** global configuration command.

The ENABLE_BREAK environment variable can also be reset by using the **no boot enable-break** global configuration command.

The HELPER environment variable can also be reset by using the **no boot helper** global configuration command.

The CONFIG_FILE environment variable can also be reset by using the **no boot config-file** global configuration command.

Examples

This example shows how to reset the prompt string to its previous setting:

```
controller# unset PS1
```

Related Commands

Command	Description
set	Sets or displays environment variables.

version

To display the boot loader version, use the **version** command in boot loader mode.

version

Command Default

None

Command Modes

Boot loader

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to display the boot loader version on a controller:

```
Controller# version
C3850 Boot Loader (C3850-HBOOT-M) Version 1.1, RELEASE SOFTWARE (P)
Compiled Fri Nov 16 06:32:46 PST 2012 by rel
```

wireless client

To configure client parameters, use the **wireless client** command.

wireless client {**association limit** *assoc-number* **interval** *interval*| **band-select** {**client-rssi** *rssi*| **cycle-count** *count*| **cycle-threshold** *threshold*| **expire dual-band** *timeout*| **expire suppression** *timeout*}| **max-user-login** *max-user-login*| **timers auth-timeout** *seconds*| **user-timeout** *user-timeout*}

Syntax Description

association limit *assoc-number* **interval** *interval*	Enables association request limit per access point slot at a given interval and configures the association request limit interval. You can configure number of association request per access point slot at a given interval from one through 100. You can configure client association request limit interval from 100 through 10000 milliseconds.
band-select	Configures band select options for the client.
client-rssi *rssi*	Sets the client received signal strength indicator (RSSI) threshold for band select. Minimum dBm of a client RSSI to respond to probe between -90 and -20.
cycle-count *count*	Sets the band select probe cycle count. You can configure the cycle count from one through 10.
cycle-threshold *threshold*	Sets the time threshold for a new scanning cycle. You can configure the cycle threshold from one through 1000 milliseconds.
expire dual-band *timeout*	Sets the timeout before stopping to try to push a given client to the 5-GHz band. You can configure the timeout from 10 through 300 seconds, and the default value is 60 seconds.
expire suppression *timeout*	Sets the expiration time for pruning previously known dual-band clients. You can configure the suppression from 10 through 200 seconds, and the default timeout value is 20 seconds.
max-user-login *max-user-login*	Configures the maximum number of login sessions for a user.
timers auth-timeout *seconds*	Configures client timers.
user-timeout *user-timeout*	Configures the idle client timeout.

Command Default None

Command Modes Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples This example shows how to set the proble cycle count for band select to 8:

```
Controller# configure terminal
Controller(config)# wireless client band-select cycle-count 8
Controller(config)# end
```

This example shows how to set the time threshold for a new scanning cycle with threshold value of 700 milliseconds:

```
Controller# configure terminal
Controller(config)# wireless client band-select cycle-threshold 700
Controller(config)# end
```

This example shows how to suppress dual-band clients from the dual-band database after 70 seconds:

```
Controller# configure terminal
Controller(config)# wireless client band-select expire suppression 70
Controller(config)# end
```

wireless client mac-address deauthenticate

To disconnect a wireless client, use the **wireless client mac-address deauthenticate** command.

wirelessclientmac-address *mac-addr***deauthenticate**

Syntax Description

mac-address *mac-addr*	Wireless client MAC address.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to disconnect a wireless client:

```
Controller# configure terminal
Controller(config)# wireless client mac-address 00:1f:ca:cf:b6:60 deauthenticate
Controller(config)# end
```

wireless client mac-address

To configure the wireless client settings, use the **wireless client mac-address** command.

wireless client mac-address *mac-addr* **ccx** {**clear-reports**| **clear-results**| **default-gw-ping**| **dhcp-test**| **dns-ping**| **dns-resolve hostname** *host-name*| **get-client-capability**| **get-manufacturer-info**| **get-operating-parameters**| **get-profiles**| **log-request** {**roam**| **rsna**| **syslog**}| **send-message** *message-id*| **stats-request** *measurement-duration* {**dot11**| **security**}| **test-abort**| **test-association** *ssid bssid dot11 channel*| **test-dot1x** [*profile-id*] *bssid dot11 channel*| **test-profile** {**any**| *profile-id*}}

Syntax Description

mac-addr	MAC address of the client.
ccx	Cisco client extension (CCX).
clear-reports	Clears the client reporting information.
clear-results	Clears the test results on the controller.
default-gw-ping	Sends a request to the client to perform the default gateway ping test.
dhcp-test	Sends a request to the client to perform the DHCP test.
dns-ping	Sends a request to the client to perform the Domain Name System (DNS) server IP address ping test.
dns-resolve hostname *host-name*	Sends a request to the client to perform the Domain Name System (DNS) resolution test to the specified hostname.
get-client-capability	Sends a request to the client to send its capability information.
get-manufacturer-info	Sends a request to the client to send the manufacturer's information.
get-operating-parameters	Sends a request to the client to send its current operating parameters.
get-profiles	Sends a request to the client to send its profiles.
log-request	Configures a CCX log request for a specified client device.
roam	(Optional) Specifies the request to specify the client CCX roaming log
rsna	(Optional) Specifies the request to specify the client CCX RSNA log.
syslog	(Optional) Specifies the request to specify the client CCX system log.

send-message *message-id*

Sends a message to the client.

Message type that involves one of the following:

- 1—The SSID is invalid
- 2—The network settings are invalid.
- 3—There is a WLAN credibility mismatch.
- 4—The user credentials are incorrect.
- 5—Please call support.
- 6—The problem is resolved.
- 7—The problem has not been resolved.
- 8—Please try again later.
- 9—Please correct the indicated problem.
- 10—Troubleshooting is refused by the network.
- 11—Retrieving client reports.
- 12—Retrieving client logs.
- 13—Retrieval complete.
- 14—Beginning association test.
- 15—Beginning DHCP test.
- 16—Beginning network connectivity test.
- 17—Beginning DNS ping test.
- 18—Beginning name resolution test.
- 19—Beginning 802.1X authentication test.
- 20—Redirecting client to a specific profile.
- 21—Test complete.
- 22—Test passed.
- 23—Test failed.
- 24—Cancel diagnostic channel operation or select a WLAN profile to resume normal operation.
- 25—Log retrieval refused by the client.
- 26—Client report retrieval refused by the client.
- 27—Test request refused by the client.
- 28—Invalid network (IP) setting.
- 29—There is a known outage or problem with the network.
- 30—Scheduled maintenance period.

- 31—The WLAN security method is not correct.
- 32—The WLAN encryption method is not correct.
- 33—The WLAN authentication method is not correct.

stats-request *measurement-duration*	Senda a request for statistics.
dot11	Optional) Specifies dot11 counters.
security	(Optional) Specifies security counters.
test-abort	Sends a request to the client to abort the current test.
test-association *ssid bssid dot11 channel*	Sends a request to the client to perform the association test.
test-dot1x	Sends a request to the client to perform the 802.1x test.
profile-id	(Optional) Test profile name.
bssid	Basic SSID.
dot11	Specifies the 802.11a, 802.11b, or 802.11g network.
channel	Channel number.
test-profile	Sends a request to the client to perform the profile redirect test.
any	Sends a request to the client to perform the profile redirect test.
profile-id	Test profile name. **Note** The profile ID should be from one of the client profiles for which client reporting is enabled.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The **default-gw-ping** test does not require the client to use the diagnostic channel.

Examples This example shows how to clear the reporting information of the client MAC address 00:1f:ca:cf:b6:60:

```
Controller# configure terminal
Controller(config)# wireless client mac-address 00:1f:ca:cf:b6:60 ccx clear-reports
Controller(config)# end
```

wireless load-balancing

To globally configure aggressive load balancing on the controller, use the **wireless load-balancing** command.

wireless load-balancing {**denial** *denial-count*| **window** *client-count*}

Syntax Description

denial *denial-count*	Specifies the number of association denials during load balancing. Maximum number of association denials during load balancing is from 1 to 10 and the default value is 3.
window *client-count*	Specifies the aggressive load balancing client window, with the number of clients needed to trigger aggressive load balancing on a given access point. Aggressive load balancing client window with the number of clients is from 0 to 20 and the default value is 5.

Command Default

Disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Load-balancing-enabled WLANs do not support time-sensitive applications like voice and video because of roaming delays.

When you use Cisco 7921 and 7920 Wireless IP Phones with controllers, make sure that aggressive load balancing is disabled on the voice WLANs for each controller. Otherwise, the initial roam attempt by the phone might fail, causing a disruption in the audio path.

Examples

This example shows how to configure association denials during load balancing:

```
Controller# configure terminal
Controller(config)# wireless load-balancing denial 5
Controller(config)# end
```

wireless sip preferred-call-no

To add a new preferred call or configure voice prioritization, use the **wireless sip preferred-call-no** command. To remove a preferred call, use the **no** form of this command.

wireless sip preferred-call-no *callIndex call-no*

no wireless sip preferred-call-no *callIndex*

Syntax Description

callIndex	Call index with valid values between 1 and 6.
call-no	Preferred call number that can contain up to 27 characters.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Before you configure voice prioritization, you must complete the following prerequisites:

- Set WLAN QoS to allow voice calls to pass through.
- Enable ACM for the radio.
- Enable SIP call snooping on the WLAN.

Examples

This example shows how to add a new preferred call or configure voice prioritization:

```
Controller# configure terminal
Controller(config)# wireless sip preferred-call-no 2 0123456789
Controller(config)# end
```

PART II

QoS

QoS Commands

This chapter contains the following QoS commands:

class

To define a traffic classification match criteria for the specified class-map name, use the **class** command in policy-map configuration mode. Use the **no** form of this command to delete an existing class map.

class {*class-map-name* | **class-default**}

no class {*class-map-name* | **class-default**}

Syntax Description

class-map-name	Assigns a name to the class map.
class-default	Refers to a system default class that matches unclassified packets.

Command Default

No policy map class-maps are defined.

Command Modes

Policy-map configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Before using the **class** command, you must use the **policy-map** global configuration command to identify the policy map and enter policy-map configuration mode. After specifying a policy map, you can configure a policy for new classes or modify a policy for any existing classes in that policy map. You attach the policy map to a port by using the **service-policy** interface configuration command.

After entering the **class** command, you enter policy-map class configuration mode. These configuration commands are available:

- **exit—**Exits policy-map class configuration mode and returns to policy-map configuration mode.
- **no—**Returns a command to its default setting.
- **police—**Defines a policer or aggregate policer for the classified traffic. The policer specifies the bandwidth limitations and the action to take when the limits are exceeded. For more information, see police, on page 150 and police aggregate.
- **set—**Specifies a value to be assigned to the classified traffic. For more information, see
- **trust—**Defines a trust state for traffic classified with the **class** or the **class-map** command. For more information, see trust, on page 198.

To return to policy-map configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

The **class** command performs the same function as the **class-map** global configuration command. Use the **class** command when a new classification, which is not shared with any other ports, is needed. Use the **class-map** command when the map is shared among many ports.

You can configure a default class by using the **class class-default** policy-map configuration command. Unclassified traffic (traffic that does not meet the match criteria specified in the traffic classes) is treated as default traffic.

Examples

This example shows how to create a policy map called *policy1*. When attached to the ingress direction, it matches all the incoming traffic defined in *class1*, sets the IP Differentiated Services Code Point (DSCP) to 10, and polices the traffic at an average rate of 1 Mb/s and bursts at 20 KB. Traffic exceeding the profile is marked down to a DSCP value gotten from the policed-DSCP map and then sent.

```
Controller(config)# policy-map policy1
Controller(config-pmap)# class class1
Controller(config-pmap-c)# set dscp 10
Controller(config-pmap-c)# police 1000000 20000 exceed-action policed-dscp-transmit
Controller(config-pmap-c)# exit
```

This example shows how to configure a default traffic class to a policy map:

```
Controller# configure terminal
Controller(config)# class-map cm-3
Controller(config-cmap)# match ip dscp 30
Controller(config-cmap)# match protocol ipv6
Controller(config-cmap)# exit
Controller(config)# class-map cm-4
Controller(config-cmap)# match ip dscp 40
Controller(config-cmap)# match protocol ip
Controller(config-cmap)# exit
Controller(config)# policy-map pm3
Controller(config-pmap)# class class-default
Controller(config-pmap-c)# set dscp 10
Controller(config-pmap-c)# exit
Controller(config-pmap)# class cm-3
Controller(config-pmap-c) set dscp 4
Controller(config-pmap-c)# exit
Controller(config-pmap)# class cm-4
Controller(config-pmap-c)# trust cos
Controller(config-pmap-c)# exit
Controller(config-pmap)# exit
```

You can verify your settings by entering the **show policy-map** privileged EXEC command.

This example shows how the default traffic class is automatically placed at the end of policy-map pm3 even though **class-default** was configured first:

```
Controller# show policy-map pm3
  Policy Map pm3
    Class cm-3
      set dscp 4
    Class cm-4
      trust cos
    Class class-default
      set dscp 10
Controller#
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to the class whose name you specify.
police	Defines a policer for classified traffic.
policy map	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
set	Classifies IP traffic by setting a DSCP or IP-precedence value in the packet.
show policy-map	Displays quality of service (QoS) policy maps.
trust, on page 198	Defines a trust state for the traffic classified through the **class** policy-map configuration command or the **class-map** global configuration command.

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to the class whose name you specify and enters class-map configuration mode.
police	Defines a policer for classified traffic.
policy-map	Creates or modifies a policy map that can be attached to multiple physical ports or SVIs and enters policy-map configuration mode.
set	Classifies IP traffic by setting a DSCP or an IP-precedence value in the packet.
show policy-map	Displays QoS policy maps.
trust	Defines a trust state for traffic classified through the class policy-map configuration or the class-map global configuration command.

class-map

To create a class map to be used for matching packets to the class whose name you specify and to enter class-map configuration mode, use the **class-map** command in global configuration mode. Use the **no** form of this command to delete an existing class map and to return to global or policy map configuration mode.

class-map [**match-any**] *class-map-name*

no class-map [**match-any**] *class-map-name*

class-map [**match-all**| **match-any**] **class-map-name**

no class-map[**match-all**| **match-any**] **class-map-name**

Syntax Description

match-any	(Optional) Perform a logical-OR of the matching statements under this class map. One or more criteria must be matched.
class-map-name	Name of the class map.

Syntax Description

match-all	(Optional) Perform a logical-AND of all matching statements under this class map. All criteria in the class map must be matched.
match-any	(Optional) Perform a logical-OR of the matching statements under this class map. One or more criteria must be matched.
class-map-name	Name of the class map.

Command Default

No class maps are defined.

If neither the **match-all** or **match-any** keyword is specified, the default is **match-all**.

Command Modes

Global configuration

Policy map configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Use this command to specify the name of the class for which you want to create or modify class-map match criteria and to enter class-map configuration mode.

The **class-map** command and its subcommands are used to define packet classification, marking, and aggregate policing as part of a globally named service policy applied on a per-port basis.

After you are in quality of service (QoS) class-map configuration mode, these configuration commands are available:

- **description**: describes the class map (up to 200 characters). The **show class-map** privileged EXEC command displays the description and the name of the class-map.
- **exit**: exits from QoS class-map configuration mode.
- **match**: configures classification criteria. For more information, see the match (class-map configuration), on page 145 command.
- **no**: removes a match statement from a class map.
- **rename**: renames the current class map. If you rename a class map with a name that is already used, the message A class-map with this name already exists appears.

If you enter the **match-all** or **match-any** keyword, you can only use it to specify an extended named access control list (ACL) with the **match access-group** class-map configuration command.

To define packet classification on a physical-port basis, only one **match** command per class map is supported. In this situation, the **match-all** and **match-any** keywords are equivalent.

Only one ACL can be configured in a class map. The ACL can have multiple access control entries (ACEs).

Examples

This example shows how to configure the class map called class1 with one match criterion, which is an access list called 103:

```
Controller(config)# access-list 103 permit ip any any dscp 10
Controller(config)# class-map class1
Controller(config-cmap)# match access-group 103
Controller(config-cmap)# exit
```

This example shows how to delete the class map class1:

```
Controller(config)# no class-map class1
```

You can verify your settings by entering the **show class-map** privileged EXEC command.

Related Commands

Command	Description
class, on page 135	Defines a traffic classification match criteria (through the **police**, **set**, and **trust** policy-map class configuration commands) for the specified class-map name.
match (class-map configuration), on page 145	Defines the match criteria to classify traffic.
policy-map, on page 153	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
show class-map	Displays QoS class maps.

Related Commands

Command	Description
class	Defines a traffic classification match criteria for the specified class-map name.
match (class-map configuration)	Defines the match criteria to classify traffic.
policy-map	Creates or modifies a policy map that can be attached to multiple physical ports or SVIs and enters policy-map configuration mode.
show class-map	Displays QoS class maps, which define the match criteria to classify traffic.

debug platform qos-acl-tcam

To enable debugging of the quality of service (QoS) and access control list (ACL) hardware memory manager software, use the **debug platform qos-acl-tcam** command in privileged or user EXEC mode. To disable debugging, use the **no** form of this command.

debug platform qos-acl-tcam {**all** | **ctcam** | **errors** | **labels** | **mask** | **rpc** | **tcam**}

no debug platform qos-acl-tcam {**all** | **ctcam** | **errors** | **labels** | **mask** | **rpc** | **tcam**}

Syntax Description

all	Displays all QoS and ACL ternary content addressable memory (QATM) manager debug messages.
ctcam	Displays Cisco TCAM (CTCAM) related-events debug messages.
errors	Displays QATM error-related-events debug messages.
labels	Displays QATM label-related-events debug messages.
mask	Displays QATM mask-related-events debug messages.
rpc	Displays QATM remote procedure call (RPC) related-events debug messages.
tcam	Displays QATM hardware-memory-related events debug messages.

Command Default

Debugging is disabled.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The **undebug platform qos-acl-tcam** command is the same as the **no debug platform qos-acl-tcam** command.

When you enable debugging on a switch stack, it is enabled only on the active switch. To enable debugging on a stack member, you can start a session from the active switch by using the **session** *switch-number* EXEC command. Then enter the **debug** command at the command-line prompt of the stack member. You also can use the **remote command** *stack-member-number LINE* EXEC command on the active switch to enable debugging on a member switch without first starting a session.

debug qos-manager

To enable debugging of the quality of service (QoS) manager software, use the **debug qos-manager** command in privileged EXEC mode. Use the **no** form of this command to disable debugging.

debug qos-manager {**all**| **event**| **verbose**}

no debug qos-manager {**all**| **event**| **verbose**}

Syntax Description

all	Display all QoS-manager debug messages.
event	Display QoS-manager related-event debug messages.
verbose	Display QoS-manager detailed debug messages.

Command Default

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The **undebug qos-manager** command is the same as the **no debug qos-manager** command.

When you enable debugging on a switch stack, it is enabled only on the stack master. To enable debugging on a stack member, you can start a session from the stack master by using the **session** *switch-number* privileged EXEC command. Then enter the **debug** command at the command-line prompt of the stack member. You also can use the **remote command** *stack-member-number LINE* privileged EXEC command on the stack master switch to enable debugging on a member switch without first starting a session.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.

match (access-map configuration)

To set the VLAN map to match packets against one or more access lists, use the **match** command in access-map configuration mode. Use the **no** form of this command to remove the match parameters.

{**match ip address** {*name*| *number*} [*name*| *number*] [*name*| *number*]...| **mac address** *name* [*name*] [*name*]...}

{**no match ip address** {*name*| *number*} [*name*| *number*] [*name*| *number*]...| **mac address** *name* [*name*] [*name*]...}

Syntax Description

ip address	Set the access map to match packets against an IP address access list.
mac address	Set the access map to match packets against a MAC address access list.
name	Name of the access list to match packets against.
number	Number of the access list to match packets against. This option is not valid for MAC access lists.

Command Default

The default action is to have no match parameters applied to a VLAN map.

Command Modes

Access-map configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You enter access-map configuration mode by using the **vlan access-map** global configuration command.

You must enter one access list name or number; others are optional. You can match packets against one or more access lists. Matching any of the lists counts as a match of the entry.

In access-map configuration mode, use the **match** command to define the match conditions for a VLAN map applied to a VLAN. Use the **action** command to set the action that occurs when the packet matches the conditions.

Packets are matched only against access lists of the same protocol type; IP packets are matched against IP access lists, and all other packets are matched against MAC access lists.

Both IP and MAC addresses can be specified for the same map entry.

Examples

This example shows how to define and apply a VLAN access map *vmap4* to VLANs 5 and 6 that will cause the interface to drop an IP packet if the packet matches the conditions defined in access list *al2*.

```
Controller(config)# vlan access-map vmap4
Controller(config-access-map)# match ip address al2
Controller(config-access-map)# action drop
Controller(config-access-map)# exit
Controller(config)# vlan filter vmap4 vlan-list 5-6
```

You can verify your settings by entering the **show vlan access-map** privileged EXEC command.

Related Commands

Command	Description
access-list	Configures a standard numbered ACL.
action	Specifies the action to be taken if the packet matches an entry in an ACL.
ip access list	Creates a named access list.
mac access-list extended	Creates a named MAC address access list.
show vlan access-map	Displays the VLAN access maps created on the switch.
vlan access-map	Creates a VLAN access map.

match (class-map configuration)

To define the match criteria to classify traffic, use the **match** command in class-map configuration mode. Use the **no** form of this command to remove the match criteria.

match {**access-group** {**name** *acl-name* | *acl-index*} | **input-interface** *interface-id-list* | **[ip] dscp** *dscp-list* | **ip precedence** *ip-precedence-list*}

no match {**access-group** {**name** *acl-name* | *acl-index*} | **input-interface** *interface-id-list* | **[ip] dscp** *dscp-list* | **ip precedence** *ip-precedence-list*}

Syntax Description

access-group	Specify an access group.
name *acl-name*	Specify the name of an IP standard or extended access control list (ACL) or MAC ACL.
acl-index	Specify the number of an IP standard or extended access control list (ACL) or MAC ACL. For an IP standard ACL, the ACL index range is 1 to 99 and 1300 to 1999. For an IP extended ACL, the ACL index range is 100 to 199 and 2000 to 2699.
input-interface *interface-id-list*	Specify the physical ports to which the interface-level class map in a hierarchical policy map applies. This command can only be used in the child-level policy map and must be the only match condition in the child-level policy map. You can specify up to six entries in the list by specifying a port (counts as one entry), a list of ports separated by a space (each port counts as an entry), or a range of ports separated by a hyphen (counts as two entries).
ip dscp *dscp-list*	List of up to eight IP Differentiated Services Code Point (DSCP) values to match against incoming packets. Separate each value with a space. The range is 0 to 63. You also can enter a mnemonic name for a commonly-used value.
ip precedence *ip-precedence-list*	List of up to eight IP-precedence values to match against incoming packets. Separate each value with a space. The range is 0 to 7. You also can enter a mnemonic name for a commonly-used value

Command Default

No match criteria are defined.

Command Modes

Class-map configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The **match** command is used to specify which fields in the incoming packets are examined to classify the packets. Only the IP access group or the MAC access group matching to the Ether Type/Len are supported.

If you enter the **class-map match-any** class-map-name global configuration command, you can enter the following **match** commands:

- **match access-group name** *acl-name*

Note The ACL must be an extended named ACL.

- **match input-interface** *interface-id-list*
- **match ip dscp** *dscp-list*
- **match ip precedence** *ip-precedence-list*

You cannot enter the **match access-group** *acl-index* command.

To define packet classification on a physical-port basis, only one **match** command per class map is supported. In this situation, the **match-any** keyword is equivalent.

For the **match ip dscp** *dscp-list* or the **match ip precedence** *ip-precedence-list* command, you can enter a mnemonic name for a commonly used value. For example, you can enter the **match ip dscp** af11 command, which is the same as entering the **match ip dscp** 10 command. You can enter the **match ip precedence critical** command, which is the same as entering the **match ip precedence** 5 command. For a list of supported mnemonics, enter the **match ip dscp** ? or the **match ip precedence** ? command to see the command-line help strings.

Use the **input-interface** *interface-id-list* keyword when you are configuring an interface-level class map in a hierarchical policy map. For the *interface-id-list*, you can specify up to six entries.

Examples

This example shows how to create a class map called class2, which matches all the incoming traffic with DSCP values of 10, 11, and 12:

```
Controller(config)# class-map class2
Controller(config-cmap)# match ip dscp 10 11 12
Controller(config-cmap)# exit
```

This example shows how to create a class map called class3, which matches all the incoming traffic with IP-precedence values of 5, 6, and 7:

```
Controller(config)# class-map class3
Controller(config-cmap)# match ip precedence 5 6 7
Controller(config-cmap)# exit
```

This example shows how to delete the IP-precedence match criteria and to classify traffic using acl1:

```
Controller(config)# class-map class2
Controller(config-cmap)# match ip precedence 5 6 7
Controller(config-cmap)# no match ip precedence
Controller(config-cmap)# match access-group acl1
Controller(config-cmap)# exit
```

This example shows how to specify a list of physical ports to which an interface-level class map in a hierarchical policy map applies:

```
Controller(config)# class-map match-all class4
Controller(config-cmap)# match input-interface gigabitethernet2/0/1 gigabitethernet2/0/2
Controller(config-cmap)# exit
```

This example shows how to specify a range of physical ports to which an interface-level class map in a hierarchical policy map applies:

```
Controller(config)# class-map match-all class4
Controller(config-cmap)# match input-interface gigabitethernet2/0/1 - gigabitethernet2/0/5
Controller(config-cmap)# exit
```

You can verify your settings by entering the **show class-map** privileged EXEC command.

Related Commands

Command	Description
class-map, on page 138	Creates a class map to be used for matching packets to the class whose name you specify.
show class-map	Displays quality of service (QoS) class maps.

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to the class whose name you specify and enters class-map configuration mode.
match non-client-nrt	Matches non-client NRT (Non-Real-Time)
match wlan user-priority	Matches 802.11 specific values
show class-map	Displays QoS class maps, which define the match criteria to classify traffic.

match non-client-nrt

To match non-client NRT (Non-Real-Time), use the **match non-client-nrt** command in class-map configuration mode. Use the **no** form of this command to return to the default setting.

match non-client-nrt

no match non-client-nrt

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Class-map

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

None

Examples

```
Controller(config)# class-map test_1000
Controller(config-cmap)# match non-client-nrt
```

match wlan user-priority

To match 802.11 specific values, use the **match wlan user-priority wlan-value** command in class-map configuration mode. Use the **no** form of this command to return to the default setting.

match wlan user-priority *wlan-value* [*wlan-value*] [*wlan-value*] [*wlan-value*]

no match wlan user-priority *wlan-value* [*wlan-value*] [*wlan-value*] [*wlan-value*]

Syntax Description

wlan-value	Matches 802.11 specific values. Enter the user priority 802.11 TID user priority (0-7). (Optional) Enter up to three more user priority values separated by white-spaces.

Command Default

None

Command Modes

Class-map

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

None

Examples

```
Controller(config)# class-map test_1000
Controller(config-cmap)# match wlan user-priority 7
```

police

To define a policer for classified traffic, use the **police** command in policy-map class configuration mode. Use the **no** form of this command to remove an existing policer.

police *rate-bps burst-byte* [**conform-action transmit**]

no police rate-bps *burst-byte* [**conform-action transmit**]

Syntax Description

rate-bps	Specify the average traffic rate in bits per second (b/s). The range is 1000000 to 1000000000.
burst-byte	Specify the normal burst size in bytes. The range is 8000 to 1000000.
conform-action transmit	(Optional) When less than the specified rate, specify that the switch transmits the packet.

Command Default

No policers are defined.

Command Modes

Policy-map class configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

A policer defines a maximum permissible rate of transmission, a maximum burst size for transmissions, and an action to take if either maximum is exceeded.

When configuring hierarchical policy maps, you can only use the **police** policy-map command in a secondary interface-level policy map.

The port ASIC device, which controls more than one physical port, supports 256 policers on the switch (255 user-configurable policers plus 1 policer reserved for internal use). The maximum number of configurable policers supported per port is 63. Policers are allocated on demand by the software and are constrained by the hardware and ASIC boundaries. You cannot reserve policers per port. There is no guarantee that a port will be assigned to any policer.

To return to policy-map configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

Policing uses a token-bucket algorithm. You configure the bucket depth (the maximum burst that is tolerated before the bucket overflows) by using the *burst-byte* option of the **police** policy-map class configuration command or the **mls qos aggregate-policer** global configuration command. You configure how quickly (the average rate) the tokens are removed from the bucket by using the *rate-bps* option of the **police** policy-map

class configuration command or the **mls qos aggregate-policer** global configuration command. For more information, see the software configuration guide for this release.

Examples

This example shows how to configure a policer that drops packets if traffic exceeds 1 Mb/s average rate with a burst size of 20 KB. The DSCPs of incoming packets are trusted, and there is no packet modification.

```
Controller(config)# policy-map policy1
Controller(config-pmap)# class class1
Controller(config-pmap-c)# trust dscp
Controller(config-pmap-c)# police 1000000 20000 exceed-action drop
Controller(config-pmap-c)# exit
```

This example shows how to configure a policer that transmits packets if traffic is less than 1 Mb/s average rate with a burst size of 20 KB. There is no packet modification.

```
Controller(config)# class-map class1
Controller(config-cmap)# exit
Controller(config)# policy-map policy1
Controller(config-pmap)# class class1
Controller(config-pmap-c)# police 1000000 20000 conform-action transmit
Controller(config-pmap-c)# exit
```

This example shows how to configure a policer that transmits packets if traffic is less than 1 Mb/s average rate with a burst size of 20 KB. There is no packet modification. This example uses an abbreviated syntax:

```
Controller(config)# class-map class1
Controller(config-cmap)# exit
Controller(config)# policy-map policy1
Controller(config-pmap)# class class1
Controller(config-pmap-c)# police 1m 20000 conform-action transmit
Controller(config-pmap-c)# exit
```

This example shows how to configure a policer, which marks down the DSCP values with the values defined in policed-DSCP map and sends the packet:

```
Controller(config)# policy-map policy2
Controller(config-pmap)# class class2
Controller(config-pmap-c)# police 1000000 20000 exceed-action policed-dscp-transmit
Controller(config-pmap-c)# exit
```

You can verify your settings by entering the **show policy-map** privileged EXEC command.

Related Commands

Command	Description
class-map, on page 138	Create a class map to be used for matching packets to the class whose name you specify with the **class** command.
class, on page 135	Defines a traffic classification match criteria (through the **police**, **set**, and **trust** policy-map class configuration commands) for the specified class-map name.

Command	Description
mls qos map **policed-dscp**	Applies a policed-DSCP map to a DSCP-trusted port.
policy-map, on page 153	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
set	Classifies IP traffic by setting a DSCP or IP-precedence value in the packet.
show policy-map	Displays QoS policy maps.
trust	Defines a trust state for traffic classified through the **class** policy-map configuration or the **class-map** global configuration command.

Related Commands

Command	Description
class	Defines a traffic classification match criteria for the specified class-map name.
class-map	Creates a class map to be used for matching packets to the class whose name you specify and enters class-map configuration mode.
policy-map	Creates or modifies a policy map that can be attached to multiple physical ports or SVIs and enters policy-map configuration mode.
set	Classifies IP traffic by setting a DSCP or an IP-precedence value in the packet.
show policy-map	Displays QoS policy maps.
trust	Defines a trust state for traffic classified through the class policy-map configuration or the class-map global configuration command.

policy-map

To create or modify a policy map that can be attached to multiple physical ports or switch virtual interfaces (SVIs) and to enter policy-map configuration mode, use the **policy-map** command in global configuration mode. Use the **no** form of this command to delete an existing policy map and to return to global configuration mode.

policy-map *policy-map-name*

no policy-map *policy-map-name*

Syntax Description

policy-map-name	Name of the policy map.

Command Default

No policy maps are defined.

The default behavior is to set the Differentiated Services Code Point (DSCP) to 0 if the packet is an IP packet and to set the class of service (CoS) to 0 if the packet is tagged. No policing is performed.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

After entering the **policy-map** command, you enter policy-map configuration mode, and these configuration commands are available:

- **class**: defines the classification match criteria for the specified class map.
- **description**: describes the policy map (up to 200 characters).
- **exit**: exits policy-map configuration mode and returns you to global configuration mode.
- **no**: removes a previously defined policy map.
- **rename**: renames the current policy map.
- **sequence-interval**: enables sequence number capability.

To return to global configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

Before configuring policies for classes whose match criteria are defined in a class map, use the **policy-map** command to specify the name of the policy map to be created, added to, or modified. Entering the **policy-map** command also enables the policy-map configuration mode in which you can configure or modify the class policies for that policy map.

You can configure class policies in a policy map only if the classes have match criteria defined for them. To configure the match criteria for a class, use the **class-map** global configuration and **match** class-map configuration commands. You define packet classification on a physical-port basis.

Only one policy map per ingress port or SVI is supported. You can apply the same policy map to multiple physical ports or SVIs.

You can apply a nonhierarchical policy maps to physical ports or to SVIs. A nonhierarchical policy map is the same as the port-based policy maps in the controller. However, you can only apply a hierarchical policy map to SVIs.

A hierarchical policy map has two levels. The first level, the VLAN level, specifies the actions to be taken against a traffic flow on an SVI. The second level, the interface level, specifies the actions to be taken against the traffic on the physical ports that belong to the SVI and are specified in the interface-level policy map.

In a primary VLAN-level policy map, you can only configure the trust state or set a new DSCP or IP precedence value in the packet. In a secondary interface-level policy map, you can only configure individual policers on physical ports that belong to the SVI.

After the hierarchical policy map is attached to an SVI, an interface-level policy map cannot be modified or removed from the hierarchical policy map. A new interface-level policy map also cannot be added to the hierarchical policy map. If you want these changes to occur, the hierarchical policy map must first be removed from the SVI.

For more information about hierarchical policy maps, see the the “Policing on SVIs” section in the “Configuring QoS” chapter of the software configuration guide for this release*QoS Configuration Guide (Cisco WLC 5700 Series)*.

Examples

This example shows how to create a policy map called *policy1*. When attached to the ingress port, it matches all the incoming traffic defined in *class1*, sets the IP DSCP to 10, and polices the traffic at an average rate of 1 Mb/s and bursts at 20 KB. Traffic less than the profile is sent.

```
Controller(config)# policy-map policy1
Controller(config-pmap)# class class1
Controller(config-pmap-c)# set dscp 10
Controller(config-pmap-c)# police 1000000 20000 conform-action transmit
Controller(config-pmap-c)# exit
```

This example shows how to create a hierarchical policy map and attach it to an SVI:

```
Controller(config)# class-map cm-non-int
Controller(config-cmap)# match access-group 101
Controller(config-cmap)# exit
Controller(config)# class-map cm-non-int-2
Controller(config-cmap)# match access-group 102
Controller(config-cmap)# exit
Controller(config)# class-map cm-test-int
Controller(config-cmap)# match input-interface gigabitethernet2/0/2 - gigabitethernet2/0/3
Controller(config-cmap)# exit
Controller(config)# policy-map pm-test-int
Controller(config-pmap)# class cm-test-int
Controller(config-pmap-c)# police 18000000 8000 exceed-action drop
Controller(config-pmap-c)# exit
Controller(config-pmap)# exit
Controller(config)# policy-map pm-test-pm-2
Controller(config-pmap)# class cm-non-int
Controller(config-pmap-c)# set dscp 7
Controller(config-pmap-c)# service-policy pm-test-int
Controller(config-pmap)# class cm-non-int-2
Controller(config-pmap-c)# set dscp 15
Controller(config-pmap-c)# service-policy pm-test-int
```

```
Controller(config-pmap-c)# end
Controller(config-cmap)# exit
Controller(config)# interface vlan 10
Controller(config-if)# service-policy input pm-test-pm-2
```

This example shows how to delete *policymap2*:

```
Controller(config)# no policy-map policymap2
```

You can verify your settings by entering the **show policy-map** privileged EXEC command.

Related Commands

Command	Description
class, on page 135	Defines a traffic classification match criteria (through the **police**, **set**, and **trust** policy-map class configuration command) for the specified class-map name.
class-map, on page 138	Creates a class map to be used for matching packets to the class whose name you specify.
service-policy	Applies a policy map to a port.
show mls qos vlan	Displays the QoS policy maps attached to an SVI.
show policy-map	Displays QoS policy maps.

Related Commands

Command	Description
class	Defines a traffic classification match criteria for the specified class-map name.
class-map	Creates a class map to be used for matching packets to the class whose name you specify and enters class-map configuration mode.
service-policy	Applies a policy map to the input of a physical port or an SVI.
show policy-map	Displays QoS policy maps.

priority-queue

To enable the egress expedite queue on a port, use the **priority-queue** command in interface configuration mode. Use the **no** form of this command to return to the default setting.

priority-queue out

no priority-queue out

Syntax Description

out	Enable the egress expedite queue.

Command Default

The egress expedite queue is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
	This command was introduced.

Usage Guidelines

When you configure the **priority-queue out** command, the shaped round robin (SRR) weight ratios are affected because there is one fewer queue participating in SRR. This means that *weight1* in the **srr-queue bandwidth shape** or the **srr-queue bandwidth shape** interface configuration command is ignored (not used in the ratio calculation). The expedite queue is a priority queue, and it is serviced until empty before the other queues are serviced.

Follow these guidelines when the expedite queue is enabled or the egress queues are serviced based on their SRR weights:

- If the egress expedite queue is enabled, it overrides the SRR shaped and shared weights for queue 1.
- If the egress expedite queue is disabled and the SRR shaped and shared weights are configured, the shaped mode overrides the shared mode for queue 1, and SRR services this queue in shaped mode.
- If the egress expedite queue is disabled and the SRR shaped weights are not configured, SRR services the queue in shared mode.

Examples

This example shows how to enable the egress expedite queue when the SRR weights are configured. The egress expedite queue overrides the configured SRR weights.

```
Controller(config)# interface gigabitethernet1/0/2
Controller(config-if)# srr-queue bandwidth shape 25 0 0 0
Controller(config-if)# srr-queue bandwidth share 30 20 25 25
Controller(config-if)# priority-queue out
```

This example shows how to disable the egress expedite queue after the SRR shaped and shared weights are configured. The shaped mode overrides the shared mode.

```
Controller(config)# interface gigabitethernet1/0/2
Controller(config-if)# srr-queue bandwidth shape 25 0 0 0
Controller(config-if)# srr-queue bandwidth share 30 20 25 25
Controller(config-if)# no priority-queue out
```

You can verify your settings by entering the **show mls qos interface** *interface-id* **queueing** or the **show running-config** privileged EXEC command.

Related Commands

Command	Description
show mls qos interface queueing	Displays the queueing strategy (SRR, priority queueing), the weights corresponding to the queues, and the CoS-to-egress-queue map.
srr-queue bandwidth shape	Assigns the shaped weights and enables bandwidth shaping on the four egress queues mapped to a port.
srr-queue bandwidth share	Assigns the shared weights and enables bandwidth sharing on the four egress queues mapped to a port.

priority

To assign priority to a class of traffic belonging to a policy map, use the **priority** command in policy-map class configuration mode. To remove a previously specified priority for a class, use the **no** form of this command.

priority [**level** *level-value*]

no priority [**level** *level-value*]

priority [*Kb/s* [*burst -in-bytes*] | **level** *level-value* [*Kb/s* [*burst -in-bytes*]] | **percent** *percentage* [*Kb/s* [*burst -in-bytes*]]]

no priority [*Kb/s* [*burst -in-bytes*] | **level** *level value* [*Kb/s* [*burst -in-bytes*]] | **percent** *percentage* [*Kb/s* [*burst -in-bytes*]]]

Syntax Description

level *level-value*	(Optional) Assigns priority level. Available values for *level-value* are 1 and 2. Level 1 is a higher priority than Level 2. Level 1 reserves bandwidth and goes first, so latency is very low. Reserve it, even if doesn't use it. Both Level 1 and 2 can reserve bandwidth.

Syntax Description

Kb/s	(Optional) Guaranteed allowed bandwidth, in kilobits per second (kbps), for the priority traffic. The amount of guaranteed bandwidth varies according to the interface and platform in use. Beyond the guaranteed bandwidth, the priority traffic will be dropped in the event of congestion to ensure that the nonpriority traffic is not starved. The value must be between 1 and 2,000,000 kbps.
burst -in-bytes	(Optional) Burst size in bytes. The burst size configures the network to accommodate temporary bursts of traffic. The default burst value, which is computed as 200 milliseconds of traffic at the configured bandwidth rate, is used when theburst argument is not specified. The range of the burst is from 32 to 2000000 bytes.

level *level-value*	(Optional) Assigns priority level. Available values for *level-value* are 1 and 2. Level 1 is a higher priority than Level 2. Level 1 reserves bandwidth and goes first, so latency is very low. Reserve it , even if doesn't use it. Both Level 1 and 2 can reserve bandwidth.
percent *percentage*	Specifies that the amount of guaranteed bandwidth will be specified by the percent of available bandwidth.

Command Default

No priority is set.

Command Modes

Policy-map class configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

This command configures low latency queuing (LLQ), providing strict priority queuing (PQ) for class-based weighted fair queuing (CBWFQ). Strict PQ allows delay-sensitive data such as voice to be dequeued and sent before packets in other queues are dequeued.

The priority command allows you to set up classes based on a variety of criteria (not just User Datagram Ports [UDP] ports) and assign priority to them, and is available for use on serial interfaces and ATM permanent virtual circuits (PVCs). A similar command, the **ip rtp priority** command, allows you to stipulate priority flows based only on UDP port numbers and is not available for ATM PVCs.

When the device is not congested, the priority class traffic is allowed to exceed its allocated bandwidth. When the device is congested, the priority class traffic above the allocated bandwidth is discarded.

The bandwidth and priority commands cannot be used in the same class, within the same policy map. These commands can be used together in the same policy map, however.

Within a policy map, you can give one or more classes priority status. When multiple classes within a single policy map are configured as priority classes, all traffic from these classes is queued to the same, single, priority queue.

When the policy map containing class policy configurations is attached to the interface to stipulate the service policy for that interface, available bandwidth is assessed. If a policy map cannot be attached to a particular interface because of insufficient interface bandwidth, the policy is removed from all interfaces to which it was successfully attached.

For more information on bandwidth allocation, see the chapter "Congestion Management Overview" in the Cisco IOS Quality of Service Solutions Configuration Guide*QoS Configuration Guide (Cisco WLC 5700 Series)*.

Examples

The following example shows how to configure the priority of the voice class in policy map policy1 to Level 1:

```
Controller(config)# policy-map policy1
Controller(config-pmap)# class voice
Controller(config-pmap-c)# priority level 1
Controller(config-pmap-c)# police 1m
```

queue-buffers ratio

To configure the queue buffer for the class, use the **queue-buffers ratio** command in policy-map class configuration mode. Use the **no** form of this command to remove the ratio limit.

queue-buffers ratio *ratio limit*

no queue-buffers ratio *ratio limit*

Syntax Description

ratio limit	(Optional) Configures the queue buffer for the class. Enter the queue buffers ratio limit (0-100).

Command Default

No queue buffer for the class is defined.

Command Modes

Policy-map class configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Either **bandwidth**, **shape**, or **priority** command must be used before using this command.

The controller allows you to allocate buffers to queues. If there is no allocation made to buffers, then they are divided equally for all queues. You can use the queue-buffer ratio to divide it in a particular ratio. Since by default DTS (Dynamic Threshold and Scaling) is active on all queues, these are soft buffers.

Note The queue-buffer ratio is supported on both wired and wireless ports, but the queue-buffer ratio cannot be configured with a queue-limit.

Examples

The following example sets the queue buffers ratio to 10%:

```
Controller(config)# policy-map policy_queuebuf01
Controller(config-pmap)# class-map class_queuebuf01
Controller(config-cmap)# exit
Controller(config)# policy policy_queuebuf01
Controller(config-pmap)# class class_queuebuf01
Controller(config-pmap-c)# bandwidth percent 80
Controller(config-pmap-c)# queue-buffers ratio 10
Controller(config-pmap)# end
```

You can verify your settings by entering the **show policy-map** privileged EXEC command.

queue-limit

To specify or modify the maximum number of packets the queue can hold for a class policy configured in a policy map, use the queue-limit policy-map class configuration command. To remove the queue packet limit from a class, use the no form of this command.

queue-limit {**dscp** | **cos**} {*codepoint-value*} *percentage-of-packets*

no queue-limit {**dscp** | **cos**} {*codepoint-value*} *percentage-of-packets*

Syntax Description

dscp	Parameters for each dscp value.
cos	Parameters for each cos value.
codepoint-value	A value in the range 0 to 63 specifying the differentiated services codepoint value for the type of queue limit.
percentage-of-packets	A percentage in the range 1 to 100 specifying the maximum percentage of packets that the queue for this class can accumulate.

Command Default

None

Command Modes

Policy-map class configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Weighted fair queueing (WFQ) creates a queue for every class for which a class map is defined. Packets satisfying the match criteria for a class accumulate in the queue reserved for the class until they are sent, which occurs when the queue is serviced by the fair queueing process. When the maximum packet threshold you defined for the class is reached, enqueueing of any further packets to the class queue causes tail drop or, if Weighted Random Early Detection (WRED) is configured for the class policy, packet drop to take effect.

You use queue limits to configure Weighted Tail Drop (WTD). WTD ensures the configuration of more than one threshold per queue. Each class of service is dropped at a different threshold value to provide for QoS differentiation.

Examples

The following example configures a policy map called port-queue to contain policy for a class called dscp-1. The policy for this class is set so that the queue reserved for it has a maximum packet limit of 20%:

```
Controller(config)# policy-map policy11
Controller(config-pmap)# class dscp-1
```

```
Controller(config-pmap-c)# bandwidth percent 20
Controller(config-pmap-c)# queue-limit dscp 1 percent 20
```

queue-set

To map a port to a queue-set, use the **queue-set** command in interface configuration mode. Use the **no** form of this command to return to the default setting.

queue-set *qset-id*

no queue-set *qset-id*

Syntax Description

qset-id	Sets the ID of the queue-set. Each port belongs to a queue-set, which defines all the characteristics of the four egress queues per port. The range is 1 to 2.

Command Default

The queue-set ID is 1.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

None

Examples

This example shows how to map a port to queue-set 2:

```
Controller(config)# interface gigabitethernet2/0/1
Controller(config-if)# queue-set 2
```

You can verify your settings by entering the **show mls qos interface** [*interface-id*] **buffers** privileged EXEC command.

Related Commands

Command	Description
mls qos queue-set output buffers	Allocates buffers to a queue-set.
mls qos queue-set output threshold	Configures the weighted tail-drop (WTD) thresholds, guarantees the availability of buffers, and configures the maximum memory allocation to a queue-set.
show mls qos interface	Displays quality of service (QoS) information.

service-policy

To apply a policy map to the input of a physical port or a switch virtual interface (SVI), use the **service-policy** command in interface configuration mode. Use the **no** form of this command to remove the policy map and port association.

service-policy {**input** | **output**} *policy-map-name*

no service-policy {**input** | **output**} *policy-map-name*

Syntax Description

input *policy-map-name*	Apply the specified policy map to the input of a physical port or an SVI.
output *policy-map-name*	Apply the specified policy map to the output of a physical port or an SVI.

Command Default

No policy maps are attached to the port.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

A policy map is defined by the **policy map** command.

Only one policy map is supported per port, per direction. In other words, only one input policy and one output policy is allowed on any one port.

Only one policy map is supported on an ingress port.

Policy maps can be configured on physical ports or on SVIs. When VLAN-based quality of service (QoS) is disabled by using the **no mls qos vlan-based** interface configuration command on a physical port, you can configure a port-based policy map on the port. If VLAN-based QoS is enabled by using the **mls qos vlan-based** interface configuration command on a physical port, the switch removes the previously configured port-based policy map. After a hierarchical policy map is configured and applied on an SVI, the interface-level policy map takes effect on the interface.

You can apply a policy map to incoming traffic on a physical port or on an SVI. You can configure different interface-level policy maps for each class defined in the VLAN-level policy map. For more information about hierarchical policy maps, see the “Configuring QoS” chapter in the software configuration guide for this release*QoS Configuration Guide (Cisco WLC 5700 Series)*.

Classification using a port trust state (for example, **mls qos trust** [**cos** | **dscp** | **ip-precedence**] and a policy map (for example, **service-policy input** *policy-map-name*) are mutually exclusive. The last one configured overwrites the previous configuration.

Note Though visible in the command-line help strings, the **history** keyword is not supported, and you should ignore the statistics that it gathers. The **output** keyword is also not supported.

Examples

This example shows how to apply plcmap1 to an physical ingress port:

```
Controller(config)# interface gigabitethernet2/0/1
Controller(config-if)# service-policy input plcmap1
```

This example shows how to remove plcmap2 from a physical port:

```
Controller(config)# interface gigabitethernet2/0/2
Controller(config-if)# no service-policy input plcmap2
```

The following example displays a VLAN policer configuration. At the end of this configuration, the VLAN policy map is applied to an interface for QoS:

```
Controller# configure terminal
Controller(config)# class-map vlan100
Controller(config-cmap)# match vlan 100
Controller(config-cmap)# exit
Controller(config)# policy-map vlan100
Controller(config-pmap)# policy-map class vlan100
Controller(config-pmap-c)# police 100000 bc conform-action transmit exceed-action drop
Controller(config-pmap-c-police)# end
Controller# configure terminal
Controller(config)# interface gigabitEthernet1/0/5
Controller(config-if)#  service-policy input vlan100
```

This example shows how to apply *plcmap1* to an ingress SVI when VLAN-based QoS is enabled:

```
Controller(config)# interface vlan 10
Controller(config-if)# service-policy input plcmap1
```

This example shows how to create a hierarchical policy map and attach it to an SVI:

```
Controller# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Controller(config)# access-list 101 permit ip any any
Controller(config)# class-map cm-1
Controller(config-cmap)# match access 101
Controller(config-cmap)# exit
Controller(config)# exit
Controller# config t
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)# class-map cm-interface-1
Controller(config-cmap)# match input gigabitethernet3/0/1 - gigabitethernet3/0/2
Controller(config-cmap)# exit
Controller(config)# policy-map port-plcmap
Controller(config-pmap)# class-map cm-interface-1
Controller(config-pmap-c)# police 900000 9000 exc policed-dscp-transmit
Controller(config-pmap-c)# exit
Controller(config-pmap)# exit
Controller(config)# policy-map vlan-plcmap
Controller(config-pmap)# class-map cm-1
```

```
Controller(config-pmap-c)# set dscp 7
Controller(config-pmap-c)# service-policy port-plcmap-1
Controller(config-pmap-c)# exit
Controller(config-pmap)# class-map cm-2
Controller(config-pmap-c)# match ip dscp 2
Controller(config-pmap-c)# service-policy port-plcmap-1
Controller(config-pmap)# exit
Controller(config-pmap)# class-map cm-3
Controller(config-pmap-c)# match ip dscp 3
Controller(config-pmap-c)# service-policy port-plcmap-2
Controller(config-pmap)# exit
Controller(config-pmap)# class-map cm-4
Controller(config-pmap-c)# trust dscp
Controller(config-pmap)# exit
Controller(config)# int vlan 10
Controller(config-if)#
Controller(config-if)# ser input vlan-plcmap
Controller(config-if)# exit
Controller(config)# exit
Controller#
```

You can verify your settings by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
policy-map	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
show policy-map, on page 196	Displays QoS policy maps.
show running-config	Displays the operating configuration.

Related Commands

Command	Description
policy-map	Creates or modifies a policy map that can be attached to multiple physical ports or SVIs and enters policy-map configuration mode.
show policy-map	Displays QoS policy maps.

service-policy (WLAN)

To configure the WLAN quality of service (QoS) service policy, use the **service-policy** command. To disable a QoS policy on a WLAN, use the **no** form of this command.

service-policy [client] {**input| output**} *policy-name*

no service-policy [client] {**input| output**} *policy-name*

Syntax Description

client	(Optional) Assigns a policy map to all clients in the WLAN.
input	Assigns an input policy map.
output	Assigns an output policy map.
policy-name	Policy name.

Command Default

No policies are assigned and the state assigned to the policy is None.

Command Modes

wlan

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You must disable the WLAN before using this command.

Examples

This example shows how to configure the input QoS service policy on a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# service-policy input policy-test
```

This example shows how to disable the input QoS service policy on a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# no service-policy input policy-test
```

set

To classify IP traffic by setting a Differentiated Services Code Point (DSCP) or an IP-precedence value in the packet, use the **set** command in policy-map class configuration mode. Use the **no** form of this command to remove traffic classification.

set {**dscp** *new-dscp* | **cos** *cos-value* | **[ip] precedence** *new-precedence* | **qos-group** *qos-group-value* | **wlan user-priority** *wlan-user-priority*}

no set {**dscp** *new-dscp* | **cos** *cos-value* | **[ip] precedence** *new-precedence* | **qos-group** *qos-group-value* | **wlan user-priority** *wlan-user-priority*}

set {**dscp** *new-dscp*| **[ip] precedence** *new-precedence*}

no set {**dscp** *new-dscp*| **[ip] precedence** *new-precedence*}

Syntax Description

dscp *new-dscp*	New DSCP value assigned to the classified traffic. The range is 0 to 63. You also can enter a mnemonic name for a commonly used value.
cos *cos-value*	Assigns *cos-value* as the class of service (cos) value of the classified traffic. The range is 0 to 7. You also can enter a mnemonic name for a commonly used value.
[**ip**] **precedence** *new-precedence*	New IP-precedence value assigned to the classified traffic. The range is 0 to 7. You also can enter a mnemonic name for a commonly used value.
qos-group *qos-group-value*	Assigns *qos-group-value* as the QoS value of the classified traffic. The range is 0 to 31. You also can enter a mnemonic name for a commonly used value.
wlan user-priority *wlan-user-priority*	Assigns *wlan-user-priority* as the WLAN user priority value to the classified traffic. The range is 0 to 7. You also can enter a mnemonic name for a commonly used value.

Command Default

No traffic classification is defined.

Command Modes

Policy-map class configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

If you have used the **set ip dscp** policy-map class configuration command, the controller changes this command to **set dscp** in the controller configuration. If you enter the **set ip dscp** policy-map class configuration command, this setting appears as **set dscp** in the controller configuration.

You can use the **set ip precedence** policy-map class configuration command or the **set precedence** policy-map class configuration command. This setting appears as **set ip precedence** in the controller configuration.

The **set** command is mutually exclusive with the **trust** policy-map class configuration command within the same policy map.

For the **set dscp** *new-dscp* or the **set ip precedence** *new-precedence* command, you can enter a mnemonic name for a commonly used value. For example, you can enter the **set dscp** af11 command, which is the same as entering the **set dscp** 10 command. You can enter the **set ip precedence critical** command, which is the same as entering the **set ip precedence** 5 command. For a list of supported mnemonics, enter the **set dscp ?** or the **set ip precedence ?** command to see the command-line help strings.

To return to policy-map configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

Examples

This example shows how to assign DSCP 10 to all FTP traffic without any policers:

```
Controller(config)# policy-map policy_ftp
Controller(config-pmap)# class-map ftp_class
Controller(config-cmap)# exit
Controller(config)# policy policy_ftp
Controller(config-pmap)# class ftp_class
Controller(config-pmap-c)# set dscp 10
Controller(config-pmap)# exit
```

You can verify your settings by entering the **show policy-map** privileged EXEC command.

Related Commands

Command	Description
class	Defines a traffic classification match criteria (through the **police**, **set**, and **trust** policy-map class configuration commands) for the specified class-map name.
police	Defines a policer for classified traffic.
policy-map	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
show policy-map, on page 196	Displays QoS policy maps.
trust	Defines a trust state for traffic classified through the **class** policy-map configuration command or the **class-map** global configuration command.

Related Commands

Command	Description
class	Defines a traffic classification match criteria for the specified class-map name.
police	Defines a policer for classified traffic.
policy-map	Creates or modifies a policy map that can be attached to multiple physical ports or SVIs and enters policy-map configuration mode.
show policy-map	Displays QoS policy maps.
trust	Defines a trust state for traffic classified through the class policy-map configuration or the class-map global configuration command.

show ap name service-policy

To display service-policy information for a specific Cisco lightweight access point, use the **show ap name service-policy** command.

show ap name *ap-name* **service-policy**

Syntax Description

ap-name	Name of the Cisco lightweight access point.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to display service-policy information for a specific Cisco lightweight access point:

```
Controller# show ap name 3502b service-policy

NAME: Cisco AP    , DESCR: Cisco Wireless Access Point
PID: 3502I  ,  VID: V01,  SN: FTX1525E94A


NAME: Dot11Radio0    , DESCR: 802.11N 2.4GHz Radio
PID: UNKNOWN,  VID:  ,  SN: FOC1522BLNA


NAME: Dot11Radio1    , DESCR: 802.11N 5GHz Radio
PID: UNKNOWN,  VID:  ,  SN: FOC1522BLNA
```

show ap name dot11

To display 802.11a or 802.11b configuration information that corresponds to specific Cisco lightweight access points, use the **show ap name dot11** command.

show ap name *ap-name* **dot11** {**24ghz**| **5ghz**} {**ccx**| **cdp**| **profile**| **service-poicy output**| **stats**| **tsm** {**all**| *client-mac*}}

Syntax Description

ap-name	Name of the Cisco lightweight access point.
24ghz	Displays the 2.4 GHz band.
5ghz	Displays the 5 GHz band.
ccx	Displays the Cisco Client eXtensions (CCX) radio management status information.
cdp	Displays Cisco Discovery Protocol (CDP) information.
profile	Displays configuration and statistics of 802.11 profiling.
service-policy output	Displays downstream service policy information.
stats	Displays Cisco lightweight access point statistics.
tsm	Displays 802.11 traffic stream metrics statistics.
all	Displays the list of all access points to which the client has associations.
client-mac	MAC address of the client.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to display the service policy that is associated with the access point:

```
Controller# show ap name test-ap dot11 24ghz service-policy output

Policy Name  : test-ap1
```

```
Policy State : Installed
```

This example shows how to display the CCX RRM 802.11 configuration for a specific access point:

```
Controller# show ap name AP01 dot11 24ghz ccx
```

This example show how to display CDP information for a specific access point:

```
Controller# show ap name AP01 dot11 24ghz cdp

AP Name               AP CDP State
--------------------- --------------
AP03                  Disabled
```

This example show how to display the configuration and statistics of 802.11b profiling for a specific access point:

```
Controller# show ap name AP01 dot11 24ghz profile

 802.11b Cisco AP performance profile mode            : GLOBAL
 802.11b Cisco AP Interference threshold              : 10 %
 802.11b Cisco AP noise threshold                     : -70 dBm
 802.11b Cisco AP RF utilization threshold            : 80 %
 802.11b Cisco AP throughput threshold                : 1000000 bps
 802.11b Cisco AP clients threshold                   : 12 clients
```

This example show how to display downstream service policy information for a specific access point:

```
Controller# show ap name AP01 dot11 24ghz service-policy output

Policy Name  : def-11gn
Policy State : Installed
```

This example show how to display statistics for a specific access point:

```
Controller# show ap name AP01 dot11 24ghz stats

Number of Users................................: 0
TxFragmentCount................................: 0
MulticastTxFrameCnt............................: 0
FailedCount....................................: 0
RetryCount.....................................: 0
MultipleRetryCount.............................: 0
FrameDuplicateCount............................: 0
RtsSuccessCount................................: 0
RtsFailureCount................................: 0
AckFailureCount................................: 0
RxIncompleteFragment...........................: 0
MulticastRxFrameCnt............................: 0
FcsErrorCount..................................: 0
TxFrameCount...................................: 0
WepUndecryptableCount..........................: 0
TxFramesDropped................................: 0

Call Admission Control (CAC) Stats
  Voice Bandwidth in use(% of config bw).........: 0
  Video Bandwidth in use(% of config bw).........: 0
  Total BW in use for Voice(%)...................: 0
  Total BW in use for SIP Preferred call(%)......: 0

Load based Voice Call Stats
  Total channel MT free..........................: 0
  Total voice MT free............................: 0
  Na Direct......................................: 0
  Na Roam........................................: 0

WMM TSPEC CAC Call Stats
  Total num of voice calls in progress...........: 0
  Num of roaming voice calls in progress.........: 0
  Total Num of voice calls since AP joined.......: 0
  Total Num of roaming calls since AP joined.....: 0
```

```
  Total Num of exp bw requests received.....: 0
  Total Num of exp bw requests admitted.....: 0
  Num of voice calls rejected since AP joined....: 0
  Num of roam calls rejected since AP joined.....: 0
  Num of calls rejected due to insufficent bw....: 0
  Num of calls rejected due to invalid params....: 0
  Num of calls rejected due to PHY rate.....: 0
  Num of calls rejected due to QoS policy.....: 0

SIP CAC Call Stats
  Total Num of calls in progress.....: 0
  Num of roaming calls in progress.....: 0
  Total Num of calls since AP joined.....: 0
  Total Num of roaming calls since AP joined.....: 0
  Total Num of Preferred calls received.....: 0
  Total Num of Preferred calls accepted.....: 0
  Total Num of ongoing Preferred calls.....: 0
  Total Num of calls rejected(Insuff BW).....: 0
  Total Num of roam calls rejected(Insuff BW)....: 0

Band Select Stats
  Num of dual band client .....: 0
  Num of dual band client added.....: 0
  Num of dual band client expired .....: 0
  Num of dual band client replaced.....: 0
  Num of dual band client detected .....: 0
  Num of suppressed client .....: 0
  Num of suppressed client expired.....: 0
  Num of suppressed client replaced.....: 0
```

This example show how to display the traffic stream configuration for all clients that correspond to a specific access point:

```
Controller# show ap name AP01 dot11 24ghz tsm all
```

show class-map

To display quality of service (QoS) class maps, which define the match criteria to classify traffic, use the **show class-map** command in EXEC mode.

show class-map [*class-map-name*]

Syntax Description

class-map-name	(Optional) Displays the contents of the specified class map.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This is an example of output from the **show class-map** command:

```
Controller# show class-map

Class Map match-all videowizard_10-10-10-10 (id 2)
   Match access-group name videowizard_10-10-10-10

 Class Map match-any class-default (id 0)
   Match any
 Class Map match-all dscp5 (id 3)
   Match ip dscp 5
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to the class whose name you specify and enters class-map configuration mode.
match (class-map configuration)	Defines the match criteria to classify traffic.

show platform qos

To display platform-dependent quality of service (QoS) information, use the **show platform qos** command in privileged EXEC mode.

show platform qos {**advanced** | **dscp-cos counters** | **policies** | **policy** | **queue** | **trust-data** | **wireless**}

Syntax Description

advanced	Displays advanced QoS information. For information on sub-commands, see **Related Topics** below.
policer {**parameters asic** *number* | **port alloc** *number* **asic** *number*}	Displays policer information. The keywords have these meanings: • **parameters asic** *number*—Displays parameter information for the specified ASIC. The range is 0 to 1. • **port alloc** *number* **asic** *number*—Displays port allocation information for the specified port and ASIC. The port allocation range is 0 to 25. The ASIC range is 0 to 1.

Syntax Description

advanced	Displays advanced QoS information. For information on sub-commands, see **Related Topics** below.
dscp-cos counters	Displays per-port per DSCP-CoS counters. For information on sub-commands, see **Related Topics** below.
policies	Displays policies information. For information on sub-commands, see **Related Topics** below.
policy	Displays policy information. For information on sub-commands, see **Related Topics** below.
queue	Displays port queue information. For information on sub-commands, see **Related Topics** below.
trust-data	Displays platform QoS trust data. For information on sub-commands, see **Related Topics** below.
wireless	Displays wireless targets. For information on sub-commands, see **Related Topics** below.

Command Modes Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

See **Related Topics** below.

Use this command only when you are working directly with your technical support representative while troubleshooting a problem. Do not use this command unless your technical support representative asks you to do so.

Related Commands

Command	Description
show platform qos advanced	Displays advanced QoS information.
show platform qos dscp-cos counters	Displays per-port per DSCP-CoS counters
show platform qos policies	Displays the summary of policies attached to the specified target
show platform qos policy	Displays QoS policy information.
show platform qos queue	Displays port queue information
show platform qos trust-data	Displays platform QoS trust data
show platform qos wireless	Displays wireless targets

show platform qos advanced

To display advanced QoS information., use the **show platform qos advanced** command in privileged EXEC mode.

show platform qos advanced {**hwres** | **nfl entry** | **qsb** {**GigabitEthernet** *interface-id* | **TenGigabitEthernet** *interface-id* | *name*} | **qthm hier** }

Syntax Description

hwres	hardware resource information
nfl entry	Cisco NetFlow information
qsb	QoS sub-block information
GigabitEthernet	GigabitEthernet IEEE 802.3z Interface
interface-id	Specifies the ID of the QSB interface.
TenGigabitEthernet	Ten Gigabit Ethernet Interface
name	specific QoS sub-block
qthm hier	QoS target hierarchy

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

None

Examples

The following example shows the number of hardware resources that have been utilized in the system. It displays this information on a per-ASIC basis:

```
Controller# show platform qos advanced hwres

ASIC #0
Free AG Policers = 2048
Total AG Policers = 2048
Free MF Policers = 8192
Total MF Policers = 8192
```

```
Addable CLIENT-IN TCAM Entries = 956
Addable CLIENT-OUT TCAM Entries = 956
Addable SSID-IN TCAM Entries = 928
Addable SSID-OUT TCAM Entries = 928
ASIC #1
Free AG Policers = 0
Total AG Policers = 0
Free MF Policers = 0
Total MF Policers = 0
Addable CLIENT-IN TCAM Entries = 0
Addable CLIENT-OUT TCAM Entries = 0
Addable SSID-IN TCAM Entries = 0
Addable SSID-OUT TCAM Entries = 0
```

show platform qos dscp-cos counters

To displays per-port per DSCP-CoS counters, use the **show platform qos dscp-cos counters** command in privileged EXEC mode.

show platform qos dscp-cos counters {**GigabitEthernet** *interface-id* | **TenGigabitEthernet** *interface-id* | *name*}

Syntax Description

GigabitEthernet	GigabitEthernet IEEE 802.3z Interface
interface-id	Specifies the ID of the interface to be counted.
TenGigabitEthernet	Ten Gigabit Ethernet Interface
name	specific QoS sub-block

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

None

Examples

The following example displays dscp-cos counters for the specified port:

```
Controller# show platform qos dscp-cos counters gigabitEthernet1/0/1

Ingress DSCP0 0              0
Ingress DSCP1 0              0
Ingress DSCP2 0              0
Ingress DSCP3 0              0
Ingress DSCP4 0              0
Ingress DSCP5 0              0
...
Ingress DSCP63 0               0
Ingress COS0 0              0
Ingress COS1 0              0
Ingress COS2 0              0
..
Ingress COS7 0              0
Egress DSCP0 0              0
Egress DSCP1 0              0
...
Egress DSCP63 0              0
```

```
Egress COS0 0             0
Egress COS1 0             0
Egress COS2 0             0
...
```

show platform qos internal table

To display QoS internal information., use the **show platform qos internal table** command in privileged EXEC mode.

show platform qos internal table {**egress-map** *map-index* | **ingress-map** *map-index* | **markdown-entries** | **policer-map** *map-index* | **token-handle-hash-map**}

Syntax Description

egress-map	Egress map table
ingress-map	Ingress map table
markdown-entries	Markdown entries table
policer-map	Policer map table
token-handle-hash-map	Token map table
map-index	Map table index. (0-15) (0-63 for policer map)

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

None

Examples

None

show platform qos policies

To display the summary of policies attached to the specified target, use the **show platform qos policies** command in privileged EXEC mode.

show platform qos policies {**CLIENT** | **PORT** | **RADIO** | **SSID**}

Syntax Description

CLIENT	Displays the target type wireless client.
PORT	Displays the target type port.
RADIO	Displays the target type wireless radio.
SSID	Displays the target type wireless SSID.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

None

Examples

The following example displays the RADIO policies:

```
Controller#show platform qos policies RADIO
 Interface      Policy  Direction       Iif ID  State
---------       ------  ---------       ------  ------
R437619371750196 71      def-11an        OUT     0x009b794000000097      INSTALLED IN HW
R536448974412842 44      def-11an        OUT     0x00be95c000000094      INSTALLED IN HW
R489774705813751 21      def-11an        OUT     0x00ae00c000000091      INSTALLED IN HW
R446687593900279 18      def-11an        OUT     0x009eb2000000008e      INSTALLED IN HW
R443537493086700 91      def-11an        OUT     0x009d93800000008b      INSTALLED IN HW
R504343234881783 12      def-11an        OUT     0x00b32dc000000088      INSTALLED IN HW
R472864216978556 21      def-11an        OUT     0x00a7fec000000085      INSTALLED IN HW
R385411810884322 58      def-11an        OUT     0x0088ed0000000082      INSTALLED IN HW
R444587526691226 87      def-11an        OUT     0x009df3000000007f      INSTALLED IN HW
R522127835461059 80      def-11an        OUT     0x00b97f400000007c      INSTALLED IN HW
```

show platform qos policy

To displays QoS policy information, use the **show platform qos policy** command in privileged EXEC mode.

show platform qos policy {**hw_state target** *policy-target* | **name** *policy-name* | **target** *policy-target*}

Syntax Description

hw_state	Policy programmed state in hardware
name	Policy name
target	Policy target
policy-name	Policy name
policy-target	Policy target

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

None

Examples

None

show platform qos queue

To display port queue information, use the **show platform qos queue** command in privileged EXEC mode.

show platform qos queue {**config** {**GigabitEthernet** *interface-id* | **TenGigabitEthernet** *interface-id* | *queue-name*} | **stats** {**GigabitEthernet** *interface-id* | **TenGigabitEthernet** *interface-id* | *queue-name* | **internal**} }

Syntax Description

config	Configuration information
GigabitEthernet	GigabitEthernet IEEE 802.3z Interface
interface-id	Specifies the ID of the interface to be displayed.
TenGigabitEthernet	Ten Gigabit Ethernet Interface
queue-name	QoS queue name
stats	Queue statistics
internal	Internal queue statistics

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

None

Examples

The following example displays Port Queue Configuration Information:

```
Controller# show platform qos queue config GigabitEthernet1/0/1

DATA Port:21 GPN:1 AFD:Disabled QoSMap:0 HW Queues: 168 - 175
  DrainFast:Disabled PortSoftStart:1 - 600
------------------------------------------------------------
  DTS Hardmax   Softmax  PortSMin GlblSMin  PortStEnd
  --- --------  -------- -------- --------- ---------
 0   1  5     67  6   268  0      0   0      0   0   800
 1   1  4      0  7   400  2    476   2    100   2   800
 2   1  4      0  5     0  0      0   0      0   0   800
 3   1  4      0  5     0  0      0   0      0   0   800
```

```
4   1  4      0  5      0  0      0   0      0   0   800
5   1  4      0  5      0  0      0   0      0   0   800
6   1  4      0  5      0  0      0   0      0   0   800
7   1  4      0  5      0  0      0   0      0   0   800
Priority   Shaped/shared   weight  shaping_step
--------   ------------   ------  ------------
0       0     Shared           50             0
1       0     Shared           75             0
2       0     Shared        10000             0
3       0     Shared        10000            64
4       0     Shared        10000           192
5       0     Shared        10000             0
6       0     Shared        10000           228
7       0     Shared        10000             0

   Weight0 Max_Th0 Min_Th0 Weigth1 Max_Th1 Min_Th1 Weight2 Min_th2
   ------- -------  ------  ------  ------  ------  ------  ------
0       0     266       0       0     298       0       0       0
1       0     318       0       0     356       0       0       0
2       0       0       0       0       0       0       0       0
3       0       0       0       0       0       0       0       0
4       0       0       0       0       0       0       0       0
5       0       0       0       0       0       0       0       0
6       0       0       0       0       0       0       0       0
7       0       0       0       0       0       0       0       0
```

Displaying Port Queue Statistics

```
Controller# show platform qos queue stats GigabitEthernet1/0/1

DATA Port:21 Enqueue Counters
-------------------------------
Queue Buffers Enqueue-TH0 Enqueue-TH1 Enqueue-TH2
----- ------- ----------- ----------- -----------
    0       0           0         219         429
    1       0           0           0          96
    2       0           0           0           0
    3       0           0           0           0
    4       0           0           0           0
    5       0           0           0           0
    6       0           0           0           0
    7       0           0           0           0
DATA Port:21 Drop Counters
-------------------------------
Queue Drop-TH0    Drop-TH1    Drop-TH2    SBufDrop    QebDrop
----- ----------- ----------- ----------- ----------- -----------
    0           0           0           0           0           0
    1           0           0           0           0           0
    2           0           0           0           0           0
    3           0           0           0           0           0
    4           0           0           0           0           0
    5           0           0           0           0           0
    6           0           0           0           0           0
    7           0           0           0           0           0
```

show platform qos trust-data

To display platform QoS trust data, use the **show platform qos trust-data** command in privileged EXEC mode.

show platform qos trust-data {**GigabitEthernet** | **TenGigabitEthernet**} {*interface-id*} {*switch-number**}

Syntax Description

GigabitEthernet	GigabitEthernet IEEE 802.3z Interface
TenGigabitEthernet	Ten Gigabit Ethernet Interface
interface-id	The ID of the interface for which to display trust data.
switch-number	*This is required if you are connecting to a controller stack instead of a single controller.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

None

Examples

The following example displays the trust details for Interface GigabitEthernet1/0/1 if the trust boundary is not enabled:

```
Controller# show platform qos trust-data GigabitEthernet1/0/1

Interface GigabitEthernet1/0/1 trust details...
        Trust boundary enabled:False
```

show platform qos wireless

To display wireless targets, use the **show platform qos wireless** command in privileged EXEC mode.

show platform qos wireless {**afd** {**client** | **ssid**} | **stats client** *client-name*}

Syntax Description

afd	Displays the AFD information.
client	Displays the wireless client.
ssid	Displays the wireless SSID.
stats	Displays the statistics information.
client-name	The name of wireless client.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

The following example shows the QoS wireless AFD parameters:

```
Controller# show platform qos wireless afd ssid name w9
  IF Type:SSID
  ASIC: 0
  Port: 27
  Radio: 1
  Index: 0
  Afd Max Rate: 80000
  Afd Weight: 64

Null AFD Handle for target 0x88510000000071
Null AFD Handle for target 0x8d3cc000000073
Null AFD Handle for target 0xa0650000000075
  IF Type:SSID
  ASIC: 0
  Port: 21
  Radio: 1
  Index: 1
  Afd Max Rate: 80000
  Afd Weight: 64

Null AFD Handle for target 0xbebf000000006d
```

The following example shows wireless client statistics:

```
Controller# show platform qos wireless stats client 0010.1010.0005
STATS ARE IN BYTE_COUNT FORMAT...
CLIENT 2128 ACCEPT STATS 26033560
CLIENT 2128 DROP STATS 64310
unknown
```

show wireless client calls

To display the total number of active or rejected calls on the controller, use the **show wireless client calls** command.

show wireless client calls {**active** | **rejected**}

Syntax Description

active	Displays active calls.
rejected	Displays rejected calls.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

The following is sample output from the **show wireless client calls** command:

```
Controller# show wireless client calls active

TSPEC Calls:

------------------------------------------------------------------------------
MAC Address     AP Name             Status               WLAN  Authenticated
------------------------------------------------------------------------------
0000.1515.000f    AP-2           Associated             1  Yes

SIP Calls:
------------------
Number of Active TSPEC calls on 802.11a and 802.11b/g: 1
Number of Active SIP calls on 802.11a and 802.11b/g: 0
```

show wireless client dot11

To display the total number of active or rejected calls for a specific band (2.4 Ghz or 5 Ghz), use the **show wireless client dot11** command.

show wireless client dot11 {**24ghz** | **5ghz**} **calls** {**active** | **rejected**}

Syntax Description

24ghz	Displays the 802.11b/g network.
5ghz	Displays the 802.11a network.
calls	Displays the wireless client calls.
active	Displays active calls
rejected	Displays rejected calls

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

The following is sample output from the **show wireless client dot11** command:

```
Controller# show wireless client dot11 5ghz calls active

 TSPEC Calls:
------------------


SIP Calls:
------------------
Number of Active TSPEC calls on 802.11a: 0
Number of Active SIP calls on 802.11a: 0
```

show wireless client mac-address (Call Control)

To view call control information related to clients, use the **show wireless client mac-address** command in privileged EXEC mode.

show wireless client mac-address *mac-address* **call-control call-info**

Syntax Description

mac-address	The client MAC address
call-control call-info	Displays the call control and IP-related information about a client

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to display call control and IP-related information about a client:

```
Controller# show wireless client mac-address  30e4.db41.6157 call-control call-info
Client MAC Address        : 30E4DB416157

Call 1 Statistics

Uplink IP Address         : 209.165.200.225
Downlink IP Address       : 209.165.200.226
Uplink Port               : 29052
Downlink Port             : 27538
Call ID                   : c40acb4d-3b3b0.3d27da1e-356bed03
Called Party              : sip:1011
Calling Party             : sip:1012
Priority                  : 6
Call On Hold              : false
Call Duration             : 30

Call 2 Statistics

No Active Call
```

show wireless client mac-address (TCLAS)

To view information about TCLAS and user priority, use the **show wireless client mac-address** command in privileged EXEC mode.

show wireless client mac-address *mac-address* **tclas**

Syntax Description

mac-address	The client MAC address.
tclas	Displays TCLAS and user priority-related information about a client.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to display the TCLAS and user priority-related information about a client:

```
Controller# show wireless client mac-address 30e4.db41.6157 tclas
MAC Address      UP TID Mask Source IP Addr  Dest IP Addr    SrcPort DstPort Proto
-------------------------------------------------------------------------------
30e4.db41.6157    4   4   95 167838052       2164326668      5060     5060      6
30e4.db41.6157    6   1   31 0               2164326668      0        27538    17
```

show wireless client voice diagnostics

To display wireless client voice diagnostic parameters, use the **show wireless client voice diagnostics** command.

show wireless client voice diagnostics {**qos-map** | **roam-history** | **rssi** | **status** | **tspec**}

Syntax Description

qos-map	Displays information about the QoS and DSCP mapping and packet statistics in each of the four queues: VO, VI, BE, BK. The different DSCP values are also displayed.
roam-history	Displays information about the last 3 roaming histories for each known client. The output contains the timestamp, access point associated with roaming, roaming reason, and if there is a roaming failure, a reason for the roaming-failure.
rssi	Displays the client's RSSI values in the last 5 seconds when voice diagnostics are enabled.
status	Displays status of voice diagnostics for clients.
tspec	Displays if voice diagnostics are enabled for TSPEC clients.

Command Default

None

Command Modes

Privileged EXEC

Usage Guidelines

Debug voice diagnostics must be enabled for voice diagnostics to work.

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

The following is sample output from the **show wireless client voice diagnostics status** command:

```
Controller# show wireless client voice diagnostics status
Voice Diagnostics Status: FALSE
```

show policy-map

To display quality of service (QoS) policy maps, which define classification criteria for incoming traffic, use the **show policy-map** command in EXEC mode.

show policy-map [*policy-map-name*]

show policy-map [*policy-map-name* [*class class-map-name*]]

Syntax Description

policy-map-name	(Optional) Display the specified policy-map name.

Syntax Description

policy-map-name	(Optional) Display the specified policy-map name.
class *class-map-name*	(Optional) Display QoS policy actions for a individual class.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Policy maps can include policers that specify the bandwidth limitations and the action to take if the limits are exceeded.

Note Though visible in the command-line help string, the **control-plane** and **interface** keywords are not supported, and the statistics shown in the display should be ignored.

Examples

This is an example of output from the **show policy-map** command:

```
Controller# show policy-map

Policy Map videowizard_policy2
  class  videowizard_10-10-10-10
   set dscp 34
   police 100000000 2000000 exceed-action drop

 Policy Map mypolicy
```

```
class  dscp5
 set dscp 6
```

Related Commands

Command	Description
policy-map	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.

Related Commands

Command	Description
policy-map	Creates or modifies a policy map that can be attached to multiple physical ports or SVIs and enters policy-map configuration mode.

trust

To define a trust state for traffic classified through the **class** policy-map configuration or the **class-map** global configuration command, use the **trust** command in policy-map class configuration mode. Use the **no** form of this command to return to the default setting.

trust [**cos**| **dscp**| **ip-precedence**]

no trust [**cos**| **dscp**| **ip-precedence**]

Syntax Description

cos	(Optional) Classifies an ingress packet by using the packet class of service (CoS) value. For an untagged packet, the port default CoS value is used.
dscp	(Optional) Classifies an ingress packet by using the packet Differentiated Services Code Point (DSCP) values (most significant 6 bits of 8-bit service-type field). For a non-IP packet, the packet CoS value is used if the packet is tagged. If the packet is untagged, the default port CoS value is used to map CoS to DSCP.
ip-precedence	(Optional) Classifies an ingress packet by using the packet IP-precedence value (most significant 3 bits of 8-bit service-type field). For a non-IP packet, the packet CoS value is used if the packet is tagged. If the packet is untagged, the port default CoS value is used to map CoS to DSCP.

Command Default

The action is not trusted. If no keyword is specified when the command is entered, the default is **dscp**.

Command Modes

Policy-map class configuration

Command History

Release	Modification
	This command was introduced.

Usage Guidelines

Use this command to distinguish the quality of service (QoS) trust behavior for certain traffic from other traffic. For example, incoming traffic with certain DSCP values can be trusted. You can configure a class map to match and trust the DSCP values in the incoming traffic.

Trust values set with this command supersede trust values set with the **mls qos trust** interface configuration command.

The **trust** command is mutually exclusive with **set** policy-map class configuration command within the same policy map.

If you specify **trust cos**, QoS uses the received or default port CoS value and the CoS-to-DSCP map to generate a DSCP value for the packet.

If you specify **trust dscp**, QoS uses the DSCP value from the ingress packet. For non-IP packets that are tagged, QoS uses the received CoS value; for non-IP packets that are untagged, QoS uses the default port CoS value. In either case, the DSCP value for the packet is derived from the CoS-to-DSCP map.

If you specify **trust ip-precedence**, QoS uses the IP precedence value from the ingress packet and the IP-precedence-to-DSCP map. For non-IP packets that are tagged, QoS uses the received CoS value; for non-IP packets that are untagged, QoS uses the default port CoS value. In either case, the DSCP for the packet is derived from the CoS-to-DSCP map.

To return to policy-map configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

Examples

This example shows how to define a port trust state to trust incoming DSCP values for traffic classified with *class1*:

```
Controller(config)# policy-map policy1
Controller(config-pmap)# class class1
Controller(config-pmap-c)# trust dscp
Controller(config-pmap-c)# police 1000000 20000 exceed-action policed-dscp-transmit
Controller(config-pmap-c)# exit
```

You can verify your settings by entering the **show policy-map** privileged EXEC command.

Related Commands

Command	Description
class	Defines a traffic classification match criteria (through the **police**, **set**, and **trust** policy-map class configuration commands) for the specified class-map name.
police	Defines a policer for classified traffic.
policy-map	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
set	Classifies IP traffic by setting a DSCP or IP-precedence value in the packet.
show policy-map	Displays QoS policy maps.

trust device

To configure trust for supported devices connected to an interface, use the **trust device** command in interface configuration mode. Use the **no** form of this command to disable trust for the connected device.

trust device {**cisco-phone** | **cts** | **ip-camera** | **media-player**}

no trust device {**cisco-phone** | **cts** | **ip-camera** | **media-player**}

Syntax Description

cisco-phone	Cisco IP phone
cts	Cisco TelePresence System
ip-camera	IPVSC
media-player	DMP

Command Default

Trust disabled

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Use the **trust device** command on the following types of interfaces:

- **Auto—**Template Auto-Template interface
- **Capwap—**Capwap tunnel interface
- **GigabitEthernet—**GigabitEthernet IEEE 802
- **GroupVI—**Group Virtual interface
- **Internal Interface—**Internal Interface
- **Loopback—**Loopback interface
- **Null—**Null interface
- **Port-channel—**Ethernet Channel of interface
- **TenGigabitEthernet--Ten** Gigabit Ethernet
- **Tunnel—**Tunnel interface

- **Vlan—**Catalyst Vlans
- **range—**interface range command

Examples

The following example configures trust for a Cisco IP Phone in Interface GigabitEthernet 1/0/1:

```
Controller(config)# interface GigabitEthernet1/0/1
Controller(config-if)# trust device cisco-phone
```

You can verify your settings by entering the **show interface status** privileged EXEC command.

PART III

Interface

Interface Commands

This chapter displays the following commands:

-

clear nmsp statistics

To clear the Network Mobility Services Protocol (NMSP) statistics, use the **clear nmsp statistics** command in privileged EXEC mode.

clear nmsp statistics

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to clear NMSP statistics:

```
Controller# clear nmsp statistics
```

You can verify that information was deleted by entering the **show nmsp statistics** privileged EXEC command.

debug ilpower

To enable debugging of the power controller and Power over Ethernet (PoE) system, use the **debug ilpower** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug ilpower {**cdp**| **controller**| **event**| **ha**| **port**| **powerman**| **registries**| **sense**}

no debug ilpower {**cdp**| **controller**| **event**| **ha**| **port**| **powerman**| **registries**| **sense**}

Syntax Description

cdp	Displays PoE Cisco Discovery Protocol (CDP) debug messages.
controller	Displays PoE controller debug messages.
event	Displays PoE event debug messages.
ha	Displays PoE high-availability messages.
port	Displays PoE port manager debug messages.
powerman	Displays PoE power management debug messages.
registries	Displays PoE registries debug messages.
sense	Displays PoE sense debug messages.

Command Default

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

This command is supported only on PoE-capable switches.

When you enable debugging on a switch stack, it is enabled only on the stack master. To enable debugging on a stack member, you can start a session from the stack master by using the **session** *switch-number* EXEC command. Then enter the **debug** command at the command-line prompt of the stack member. You also can use the **remote command** *stack-member-number LINE* EXEC command on the stack master switch to enable debugging on a member switch without first starting a session.

debug interface

To enable debugging of interface-related activities, use the **debug interface** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug interface {*interface-id*| **counters** {**exceptions**| **protocol memory**} | **null** *interface-number*| **port-channel** *port-channel-number*| **states**|**vlan** *vlan-id*}

no debug interface {*interface-id*| **counters** {**exceptions**| **protocol memory**} | **null** *interface-number*| **port-channel** *port-channel-number*| **states**|**vlan** *vlan-id*}

Syntax Description

interface-id	ID of the physical interface. Displays debug messages for the specified physical port, identified by type switch number/module number/port, for example, gigabitethernet 1/0/2.
null *interface-number*	Displays debug messages for null interfaces. The interface number is always **0**.
port-channel *port-channel-number*	Displays debug messages for the specified EtherChannel port-channel interface. The *port-channel-number* range is 1 to 48.
vlan *vlan-id*	Displays debug messages for the specified VLAN. The vlan range is 1 to 4094.
counters	Displays counters debugging information.
exceptions	Displays debug messages when a recoverable exceptional condition occurs during the computation of the interface packet and data rate statistics.
protocol memory	Displays debug messages for memory operations of protocol counters.
states	Displays intermediary debug messages when an interface's state transitions.

Command Default

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

If you do not specify a keyword, all debug messages appear.

The **undebug interface** command is the same as the **no debug interface** command.

When you enable debugging on a switch stack, it is enabled only on the stack master. To enable debugging on a stack member, you can start a session from the stack master by using the **session** *switch-number* EXEC command. Then enter the **debug** command at the command-line prompt of the stack member. You also can use the **remote command** *stack-member-number LINE* EXEC command on the stack master switch to enable debugging on a member switch without first starting a session.

debug lldp packets

To enable debugging of Link Layer Discovery Protocol (LLDP) packets, use the **debug lldp packets** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug lldp packets

no debug lldp packets

Syntax Description

This command has no keywords or arguments.

Command Default

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The **undebug lldp packets** command is the same as the **no debug lldp packets** command.

When you enable debugging on a switch stack, it is enabled only on the . To enable debugging on a stack member, you can start a session from the by using the **session** *switch-number* EXEC command.

debug platform fallback-bridging

To enable debugging of the platform-dependent fallback bridging manager, use the **debug platform fallback-bridging** command in EXEC mode. To disable debugging, use the **no** form of this command.

debug platform fallback-bridging [**error**| **retry**| **rpc** {**events**| **messages**}]

no debug platform fallback-bridging [**error**| **retry**| **rpc** {**events**| **messages**}]

Syntax Description

error	(Optional) Displays fallback bridging manager error condition messages.
retry	(Optional) Displays fallback bridging manager retry messages.
rpc {**events** | **messages**}	(Optional) Displays fallback bridging debugging information. The keywords have these meanings: • **events—**Displays remote procedure call (RPC) events. • **messages —**Displays RPC messages.

Command Default

Debugging is disabled.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
15.0	This command was introduced.

Usage Guidelines

If you do not specify a keyword, all fallback bridging manager debug messages appear.

The **undebug platform fallback-bridging** command is the same as the **no debug platform fallback-bridging** command.

When you enable debugging on a switch stack, it is enabled only on the stack master. To enable debugging on a stack member, you can start a session from the stack master by using the **session** *switch-number* EXEC command. Then enter the **debug** command at the command-line prompt of the stack member. You also can use the **remote command** *stack-member-number LINE* EXEC command on the stack master switch to enable debugging on a member switch without first starting a session.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.

duplex

To specify the duplex mode of operation for a port, use the **duplex** command in interface configuration mode. To return to the default value, use the **no** form of this command.

duplex {**auto**| **full**| **half**}

no duplex {**auto**| **full**| **half**}

Syntax Description

auto	Enables automatic duplex configuration. The port automatically detects whether it should run in full- or half-duplex mode, depending on the attached device mode.
full	Enables full-duplex mode.
half	Enables half-duplex mode (only for interfaces operating at 10 or 100 Mb/s). You cannot configure half-duplex mode for interfaces operating at 1000 or 10,000 Mb/s.

Command Default

The default is **auto** for Fast Ethernet and Gigabit Ethernet ports.

The default is **half** for 100BASE-*x* (where -*x* is -BX, -FX, -FX-FE, or -LX) SFP modules.

Duplex options are not supported on the 1000BASE-*x* (where -*x* is -BX, -CWDM, -LX, -SX, or -ZX) small form-factor pluggable (SFP) modules.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

For Fast Ethernet ports, setting the port to **auto** has the same effect as specifying **half** if the attached device does not autonegotiate the duplex parameter.

For Gigabit Ethernet ports, setting the port to **auto** has the same effect as specifying **full** if the attached device does not autonegotiate the duplex parameter.

Note Half-duplex mode is supported on Gigabit Ethernet interfaces if the duplex mode is **auto** and the connected device is operating at half duplex. However, you cannot configure these interfaces to operate in half-duplex mode.

Certain ports can be configured to be either full duplex or half duplex. How this command is applied depends on the device to which the switch is attached.

If both ends of the line support autonegotiation, we highly recommend using the default autonegotiation settings. If one interface supports autonegotiation and the other end does not, configure duplex and speed on both interfaces, and use the **auto** setting on the supported side.

If the speed is set to **auto**, the switch negotiates with the device at the other end of the link for the speed setting and then forces the speed setting to the negotiated value. The duplex setting remains as configured on each end of the link, which could result in a duplex setting mismatch.

You can configure the duplex setting when the speed is set to **auto**.

Caution Changing the interface speed and duplex mode configuration might shut down and reenable the interface during the reconfiguration.

You can verify your setting by entering the **show interfaces** privileged EXEC command.

Examples

This example shows how to configure an interface for full-duplex operation:

```
Controller(config)# interface gigabitethernet1/0/1
Controller(config-if)# duplex full
```

interface

To configure an interface, use the **interface** command.

interface {**Auto-Template** *Auto-Template interface-number*| **Capwap** *Capwap interface-number* | **Gigabit Ethernet** *Gigabit Ethernet interface number*| **Group VI** *Group VI interface number* **Internal Interface** *Internal Interface number* **Loopback** *Loopback interface number* **Null** *Null interface* **Port-channel** *interface number***Port-channel** *interface number* **TenGigabit Ethernet** *interface number* **Tunnel** *interface number* **Vlan** *interface number*}

Syntax Description

Auto-Template *Auto-template interface-number*	Enables you to configure auto-template interface. Values range from 1 to 999.
Capwap *Capwap interface number*	Enables you to configure CAPWAP tunnel interface. Values range from 0 to 2147483647.
GigabitEthernet *Gigabit Ethernet interface number*	Enables you to configure Gigabit Ethernet IEEE 802.3z interface. Values range from 0 to 9.
Group VI *Group VI interface number*	Enables you to configure the internal interface. Values range from 0 to 9.
Internal Interface Internal Interface	Enables you to configure internal interface.
Loopback *Loopback Interface number*	Enables you to configure loopback interface. Values range from 0 to 2147483647.
Null *Null interface number*	Enables you to configure null interface. Value is 0.
Port-channel *interface number*	Enables you to configure Ethernet channel interfaces. Values range from 1 to 128.
TenGigabitEthernet *interface number*	Enables you to configure a 10-Gigabit Ethernet interface. Values range from 0 to 9.
Tunnel *interface number*	Enables you to configure the tunnel interface. Values range from 0 to 2147483647.
Vlan *interface number*	Enables you to configure switch VLAN interfaces. Values range from 0 to 4098.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You can not use the "no" form of this command.

Examples

This example shows how you can configure interface:

```
Controller# interface Tunnel 15
```

interface auto-template

To configure an auto-template interface, use the **interface auto-template** command.

interface auto-template*interface-name*

Syntax Description

interface-name	Specifies the interface number.

Command Default

Disabled

Command Modes

Global configuration mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to configure interface auto-template:

```
# interface auto-template
```

interface range

To configure an interface range, use the **interface range** command.

interface range {**Gigabit Ethernet** *interface-number* | **Loopback** *interface-number* | **Port Channel** *interface-number* | **TenGigabit Ethernet** *interface-number* **Tunnel** *interface-number* **Vlan** *interface-number* **Macro** *WORD*}

Syntax Description

GigabitEthernet *interface-number*	Configures the Gigabit Ethernet IEEE 802.3z interface. Values range from 1 to 9.
Loopback *interface-number*	Configures the loopback interface. Values range from 0 to 2147483647.
Port-Channel *interface-number*	Configures 10-Gigabit Ethernet channel of interfaces. Values range from 1 to 128.
TenGigabit Ethernet *interface-number*	Configures 10-Gigabit Ethernet interfaces. Values range from 0 to 9.
Tunnel *interface-number*	Configures the tunnel interface. Values range from 0 to 2147483647.
VLAN *interface-number*	Configures the switch VLAN interfaces. Values range from 1 to 4095.
Macro *WORD*	Configures the keywords to interfaces. Support up to 32 characters.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how you can configure interface range:

```
Controller# interface range vlan
```

location

To configure location information for an endpoint, use the **location** command in global configuration mode. To remove the location information, use the **no** form of this command.

location {**admin-tag** *string*| **civic-location identifier** {**host**| *id*}| **elin-location** *string* **identifier** *id*| **geo-location identifier** {**host**| *id*}}

no location {**admin-tag** *string*| **civic-location identifier** {**host**| *id*}| **elin-location** *string* **identifier** *id*| **geo-location identifier** {**host**| *id*}}

Syntax Description

admin-tag	Configures administrative tag or site information.
string	Site or location information in alphanumeric format.
civic-location	Configures civic location information.
identifier	Specifies the name of the civic location, emergency, or geographical location.
host	Defines the host civic or geo-spatial location.
id	Name of the civic, emergency, or geographical location. **Note** The identifier for the civic location in the LLDP-MED controller TLV is limited to 250 bytes or less. To avoid error messages about available buffer space during controller configuration, be sure that the total length of all civic-location information specified for each civic-location identifier does not exceed 250 bytes.
elin-location	Configures emergency location information (ELIN).
geo-location	Configures geo-spatial location information.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

After entering the **location civic-location identifier** global configuration command, you enter civic location configuration mode. After entering the **location geo-location identifier** global configuration command, you enter geo location configuration mode.

The civic-location identifier must not exceed 250 bytes.

The host identifier configures the host civic or geo-spatial location. If the identifier is not a host, the identifier only defines a civic location or geo-spatial template that can be referenced on the interface.

The **host** keyword defines the device location. The civic location options available for configuration using the **identifier** and the **host** keyword are the same. You can specify the following civic location options in civic location configuration mode:

- **additional-code—**Sets an additional civic location code.
- **additional-location-information—**Sets additional civic location information.
- **branch-road-name—**Sets the branch road name.
- **building—**Sets building information.
- **city—**Sets the city name.
- **country—**Sets the two-letter ISO 3166 country code.
- **county—**Sets the county name.
- **default—**Sets a command to its defaults.
- **division—**Sets the city division name.
- **exit—**Exits from the civic location configuration mode.
- **floor—**Sets the floor number.
- **landmark—**Sets landmark information.
- **leading-street-dir—**Sets the leading street direction.
- **name—**Sets the resident name.
- **neighborhood—**Sets neighborhood information.
- **no—**Negates the specified civic location data and sets the default value.
- **number—**Sets the street number.
- **post-office-box—**Sets the post office box.
- **postal-code—**Sets the postal code.
- **postal-community-name—**Sets the postal community name.
- **primary-road-name—**Sets the primary road name.
- **road-section—**Sets the road section.
- **room—**Sets room information.
- **seat—**Sets seat information.
- **state—**Sets the state name.

- **street-group—**Sets the street group.
- **street-name-postmodifier—**Sets the street name postmodifier.
- **street-name-premodifier—**Sets the street name premodifier.
- **street-number-suffix—**Sets the street number suffix.
- **street-suffix—**Sets the street suffix.
- **sub-branch-road-name—**Sets the sub-branch road name.
- **trailing-street-suffix—**Sets the trailing street suffix.
- **type-of-place—**Sets the type of place.
- **unit—**Sets the unit.

You can specify the following geo-spatial location information in geo-location configuration mode:

- **altitude—**Sets altitude information in units of floor, meters, or feet.
- **latitude—**Sets latitude information in degrees, minutes, and seconds. The range is from -90 degrees to 90 degrees. Positive numbers indicate locations north of the equator.
- **longitude—**Sets longitude information in degrees, minutes, and seconds. The range is from -180 degrees to 180 degrees. Positive numbers indicate locations east of the prime meridian.
- **resolution—**Sets the resolution for latitude and longitude. If the resolution value is not specified, default value of 10 meters is applied to latitude and longitude resolution parameters. For latitude and longitude, the resolution unit is measured in meters. The resolution value can also be a fraction.
- **default—**Sets the geographical location to its default attribute.
- **exit—**Exits from geographical location configuration mode.
- **no—**Negates the specified geographical parameters and sets the default value.

Use the **no lldp med-tlv-select location information** interface configuration command to disable the location TLV. The location TLV is enabled by default.

Examples

This example shows how to configure civic location information on the controller:

```
Controller(config)# location civic-location identifier 1
Controller(config-civic)# number 3550
Controller(config-civic)# primary-road-name "Cisco Way"
Controller(config-civic)# city "San Jose"
Controller(config-civic)# state CA
Controller(config-civic)# building 19
Controller(config-civic)# room C6
Controller(config-civic)# county "Santa Clara"
Controller(config-civic)# country US
Controller(config-civic)# end
```

You can verify your settings by entering the **show location civic-location** privileged EXEC command.

This example shows how to configure the emergency location information on the controller:

```
Controller(config)# location elin-location 14085553881 identifier 1
```

You can verify your settings by entering the **show location elin** privileged EXEC command.

The following example shows how to configure geo-spatial location information on the controller:

```
Controller(config)# location geo-location identifier host
Controller(config-geo)# latitude 12.34
Controller(config-geo)# longitude 37.23
Controller(config-geo)# altitude 5 floor
Controller(config-geo)# resolution 12.34
```

You can use the **show location geo-location identifier** command to display the configured geo-spatial location details.

logging event power-inline-status

To enable the logging of Power over Ethernet (PoE) events, use the **logging event power-inline-status** command in interface configuration mode. To disable the logging of PoE status events, use the **no** form of this command.

logging event power-inline-status

no logging event power-inline-status

Syntax Description

This command has no arguments or keywords.

Command Default

Logging of PoE events is enabled.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The **no** form of this command does not disable PoE error events.

Examples

This example shows how to enable logging of PoE events on a port:

```
Controller(config-if)# interface gigabitethernet1/0/1
Controller(config-if)# logging event power-inline-status
Controller(config-if)#
```

show CAPWAP summary

To display all the CAPWAP tunnels established by the controller to access points and other mobility controllers use the **show CAPWAP summary** command.

show CAPWAP summary

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to display CAPWAP tunnels established by the controllers to the access points and other controllers.

```
Controller# show capwap summary
CAPWAP Tunnels General Statistics:
Number of Capwap Data Tunnels = 8
Number of Capwap Mobility Tunnels = 0
Number of Capwap Multicast Tunnels = 0
Name APName Type PhyPortIf Mode McastIf
------ ------------------------------ ---- --------- ---------
-------
Ca4 AP-Behind-Router data - unicast -
Ca0 AP1142-kat data - unicast -
Ca5 APRFCHAMBER2-EDISON data - unicast -
Ca6 KATANA_2_RF data - unicast -
Ca1 AP-1040-RF data - unicast -
Ca7 KATANA_1_RF data - unicast -
Ca2 AP3500-2027 data - unicast -
Ca3 AP-1040-out data - unicast -
```

show env

To display fan, temperature, redundant power system (RPS) availability, and power information, use the **show env** command in EXEC mode.

show env {**all**| **fan**| **power** [**all**| **switch** [*stack-member-number*]]| **rps**| **stack** [*stack-member-number*] | **temperature** [**status**]}

Syntax Description

all	Displays the fan and temperature environmental status and the status of the internal power supplies and the RPS.
fan	Displays the switch fan status.
power	Displays the internal power status of the active switch.
all	(Optional) Displays the status of all the internal power supplies in a standalone switch when the command is entered on the switch, or in all the stack members when the command is entered on the stack master.
switch	(Optional) Displays the status of the internal power supplies for each switch in the stack or for the specified switch. This keyword is available only on stacking-capable switches.
stack-member-number	(Optional) Number of the stack member for which to display the status of the internal power supplies or the environmental status. The range is 1 to 9, depending on the switch member numbers in the stack.
rps	Displays the RPS status.
stack	Displays all environmental status for each switch in the stack or for the specified switch. This keyword is available only on stacking-capable switches.
temperature	Displays the switch temperature status.
status	(Optional) Displays the switch internal temperature (not the external temperature) and the threshold values.

Command Default

None

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Use the **show env** EXEC command to display the information for the switch being accessed—a standalone switch or the stack master. Use this command with the **stack** and **switch** keywords to display all information for the stack or for the specified stack member.

If you enter the **show env temperature status** command, the command output shows the switch temperature state and the threshold level.

You can also use the **show env temperature** command to display the switch temperature status. The command output shows the green and yellow states as *OK* and the red state as *FAULTY*. If you enter the **show env all** command, the command output is the same as the **show env temperature status** command output.

Examples

This is an example of output from the **show env all** command:

This is an example of output from the **show env fan** command:

This is an example of output from the **show env power all** command on the stack master:

This is an example of output from the **show env stack** command on the stack master:

This example shows how to display the temperature value, state, and the threshold values on a standalone switch. The table describes the temperature states in the command output.

Table 6: States in the show env temperature status Command Output

State	Description
Green	The switch temperature is in the *normal* operating range.
Yellow	The temperature is in the *warning* range. You should check the external temperature around the switch.
Red	The temperature is in the *critical* range. The switch might not run properly if the temperature is in this range.

show errdisable detect

To display error-disabled detection status, use the **show errdisable detect** command in EXEC mode.

show errdisable detect

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

A gbic-invalid error reason refers to an invalid small form-factor pluggable (SFP) module.

The error-disable reasons in the command output are listed in alphabetical order. The mode column shows how error-disable is configured for each feature.

You can configure error-disabled detection in these modes:

- port mode—The entire physical port is error-disabled if a violation occurs.
- vlan mode—The VLAN is error-disabled if a violation occurs.
- port/vlan mode—The entire physical port is error-disabled on some ports and is per-VLAN error-disabled on other ports.

Examples

This is an example of output from the **show errdisable detect** command:

show errdisable recovery

To display the error-disabled recovery timer information, use the **show errdisable recovery** command in EXEC mode.

show errdisable recovery

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines A gbic-invalid error-disable reason refers to an invalid small form-factor pluggable (SFP) module interface.

Note Though visible in the output, the unicast-flood field is not valid.

Examples This is an example of output from the **show errdisable recovery** command:

show interfaces

To display the administrative and operational status of all interfaces or for a specified interface, use the **show interfaces** command in privileged EXEC mode.

show interfaces [*interface-id*| **vlan** *vlan-id*] [**accounting**| **capabilities** [**module** *number*]| **debounce**| **description**| **etherchannel**| **flowcontrol**| **private-vlan mapping**| **pruning**| **stats**| **status** | **trunk**]

Syntax Description

interface-id	(Optional) ID of the interface. Valid interfaces include physical ports (including type, stack member for stacking-capable switches, module, and port number) and port channels. The port channel range is 1 to 48.
vlan *vlan-id*	(Optional) VLAN identification. The range is 1 to 4094.
accounting	(Optional) Displays accounting information on the interface, including active protocols and input and output packets and octets. **Note** The display shows only packets processed in software; hardware-switched packets do not appear.
capabilities	(Optional) Displays the capabilities of all interfaces or the specified interface, including the features and options that you can configure on the interface. Though visible in the command line help, this option is not available for VLAN IDs.
module *number*	(Optional) Displays capabilities of all interfaces on the switch or specified stack member. This option is not available if you entered a specific interface ID.
description	(Optional) Displays the administrative status and description set for an interface.
etherchannel	(Optional) Displays interface EtherChannel information.
flowcontrol	(Optional) Displays interface flow control information.
private-vlan mapping	(Optional) Displays private-VLAN mapping information for the VLAN switch virtual interfaces (SVIs). This keyword is not available if the switch is running the LAN base feature set.
pruning	(Optional) Displays trunk VTP pruning information for the interface.
stats	(Optional) Displays the input and output packets by switching the path for the interface.
status	(Optional) Displays the status of the interface. A status of unsupported in the Type field means that a non-Cisco small form-factor pluggable (SFP) module is inserted in the module slot.

err-disabled	(Optional) Displays interfaces in an error-disabled state.
trunk	(Optional) Displays interface trunk information. If you do not specify an interface, only information for active trunking ports appears.

Note Though visible in the command-line help strings, the **crb**, **fair-queue**, **irb**, **mac-accounting**, **precedence**, **random-detect**, **rate-limit**, and **shape** keywords are not supported.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The **show interfaces capabilities** command with different keywords has these results:

- Use the **show interfaces** *interface-id* **capabilities** to display the capabilities of the specified interface.
- Use the **show interfaces capabilities** (with no module number or interface ID) to display the capabilities of all interfaces in the stack.

Examples

This is an example of output from the **show interfaces** command for an interface on stack member 3:

This is an example of patrial output from the **show interfaces accounting** command:

```
Controller# show interfaces accounting
Vlan1
                Protocol    Pkts In   Chars In   Pkts Out  Chars Out
                      IP          0          0          6        378
Vlan200
                Protocol    Pkts In   Chars In   Pkts Out  Chars Out
No traffic sent or received on this interface.
GigabitEthernet0/0
                Protocol    Pkts In   Chars In   Pkts Out  Chars Out
                   Other     165476   11417844          0          0
           Spanning Tree    1240284   64494768          0          0
                     ARP       7096     425760          0          0
                     CDP      41368   18781072      82908   35318808
GigabitEthernet1/0/1
                Protocol    Pkts In   Chars In   Pkts Out  Chars Out
No traffic sent or received on this interface.
GigabitEthernet1/0/2
                Protocol    Pkts In   Chars In   Pkts Out  Chars Out
No traffic sent or received on this interface.
```

```
<output truncated>
```

This is an example of output from the **show interfaces capabilities** command for an interface:

This is an example of output from the **show interfaces** *interface* **description** command when the interface has been described as *Connects to Marketing* by using the **description** interface configuration command:

```
Controller# show interfaces gigabitethernet1/0/2 description
Interface                      Status         Protocol Description
Gi1/0/2                        up             down     Connects to Marketing
```

This is an example of output from the **show interfaces etherchannel** command when port channels are configured on the switch:

```
Controller# show interfaces etherchannel
----
Port-channel34:
Age of the Port-channel   = 28d:18h:51m:46s
Logical slot/port   = 12/34          Number of ports = 0
GC                  = 0x00000000      HotStandBy port = null
Passive port list   =
Port state          = Port-channel L3-Ag Ag-Not-Inuse
Protocol            =    -
Port security       = Disabled
```

This is an example of output from the **show interfaces private-vlan mapping** command when the private-VLAN primary VLAN is VLAN 10 and the secondary VLANs are VLANs 501 and 502:

```
Controller# show interfaces private-vlan mapping
Interface Secondary VLAN Type
--------- -------------- -----------------
vlan10    501            isolated
vlan10    502            community
```

This is an example of output from the **show interfaces** *interface-id* **pruning** command when pruning is enabled in the VTP domain:

```
Controller# show interfaces gigabitethernet1/0/2 pruning
Port      Vlans pruned for lack of request by neighbor
Gi1/0/2   3,4

Port      Vlans traffic requested of neighbor
Gi1/0/2   1-3
```

This is an example of output from the **show interfaces stats** command for a specified VLAN interface:

```
Controller# show interfaces vlan 1 stats
Switching path    Pkts In    Chars In    Pkts Out    Chars Out
     Processor    1165354   136205310      570800     91731594
   Route cache          0           0           0            0
         Total    1165354   136205310      570800     91731594
```

This is an example of partial output from the **show interfaces status** command. It displays the status of all interfaces:

```
Controller# show interfaces status
Port      Name               Status       Vlan       Duplex  Speed       Type
Gi1/0/1                      notconnect   1            auto   auto 10/100/1000Ba
seTX
Gi1/0/2                      notconnect   1            auto    100 10/100/1000Ba
seTX
Gi1/0/3                      notconnect   1            auto   1000 10/100/1000Ba
seTX
Gi1/0/4                      notconnect   1            auto   auto 10/100/1000Ba
seTX
Gi1/0/5                      notconnect   1            auto   auto 10/100/1000Ba
seTX
Gi1/0/6                      notconnect   1            auto     10 10/100/1000Ba
seTX
Gi1/0/7                      notconnect   1            auto   auto 10/100/1000Ba
```

```
seTX
Gi1/0/8                     notconnect   1            auto   auto 10/100/1000Ba
seTX
Gi1/0/9                     notconnect   1            auto   auto 10/100/1000Ba
seTX
Gi1/0/10                    notconnect   1            auto   auto 10/100/1000Ba
seTX
```

These are examples of output from the **show interfaces status** command for a specific interface when private VLANs are configured. Port 22 is configured as a private-VLAN host port. It is associated with primary VLAN 20 and secondary VLAN 25:

```
Controller# show interfaces gigabitethernet1/0/22 status
Port       Name      Status      Vlan      Duplex      Speed      Type
Gi1/0/22             connected   20,25     a-full      a-100      10/100BaseTX
```

In this example, port 20 is configured as a private-VLAN promiscuous port. The display shows only the primary VLAN 20:

```
Controller# show interfaces gigabitethernet1/0/20 status
Port       Name      Status      Vlan      Duplex      Speed      Type
Gi1/0/20             connected   20        a-full      a-100      10/100BaseTX
```

This is an example of output from the **show interfaces status err-disabled** command. It displays the status of interfaces in the error-disabled state:

```
Controller# show interfaces status err-disabled
Port      Name       Status         Reason
Gi1/0/2              err-disabled   gbic-invalid
Gi2/0/3              err-disabled   dtp-flap
```

This is an example of output from the **show interfaces** *interface-id* **pruning** command:

```
Controller# show interfaces gigabitethernet1/0/2 pruning
Port Vlans pruned for lack of request by neighbor
```

This is an example of output from the **show interfaces** *interface-id* **trunk** command. It displays trunking information for the port.

show interfaces counters

To display various counters for the switch or for a specific interface, use the **show interfaces counters** command in privileged EXEC mode.

show interfaces [*interface-id*] **counters** [**errors**| **etherchannel**| **module** *stack-member-number*| **protocol status**| **trunk**]

Syntax Description

interface-id	(Optional) ID of the physical interface, including type, stack member (stacking-capable switches only) module, and port number.
errors	(Optional) Displays error counters.
etherchannel	(Optional) Displays EtherChannel counters, including octets, broadcast packets, multicast packets, and unicast packets received and sent.
module *stack-member-number*	(Optional) Displays counters for the specified stack member. The range is from 1 to 9, depending upon the switch numbers in the stack. This keyword is available only on stacking-capable switches. **Note** In this command, the **module** keyword refers to the stack member number (1 to 9). The module number that is part of the interface ID is always zero.
protocol status	(Optional) Displays the status of protocols enabled on interfaces.
trunk	(Optional) Displays trunk counters.

Note Though visible in the command-line help string, the **vlan** *vlan-id* keyword is not supported.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

If you do not enter any keywords, all counters for all interfaces are included.

Examples

This is an example of partial output from the **show interfaces counters** command. It displays all counters for the switch.

```
Controller# show interfaces counters
Port            InOctets    InUcastPkts    InMcastPkts    InBcastPkts
Gi1/0/1                0              0              0              0
Gi1/0/2                0              0              0              0
Gi1/0/3                0              0              0              0
Gi1/0/4                0              0              0              0

<output truncated>
```

This is an example of partial output from the **show interfaces counters module** command for stack member 2. It displays all counters for the specified switch in the stack.

```
Controller# show interfaces counters module 2
Port            InOctets    InUcastPkts    InMcastPkts    InBcastPkts
Gi1/0/1              520              2              0              0
Gi1/0/2              520              2              0              0
Gi1/0/3              520              2              0              0
Gi1/0/4              520              2              0              0

<output truncated>
```

This is an example of partial output from the **show interfaces counters protocol status** command for all interfaces:

```
Controller# show interfaces counters protocol status
Protocols allocated:
Vlan1: Other, IP
Vlan20: Other, IP, ARP
Vlan30: Other, IP, ARP
Vlan40: Other, IP, ARP
Vlan50: Other, IP, ARP
Vlan60: Other, IP, ARP
Vlan70: Other, IP, ARP
Vlan80: Other, IP, ARP
Vlan90: Other, IP, ARP
Vlan900: Other, IP, ARP
Vlan3000: Other, IP
Vlan3500: Other, IP
GigabitEthernet1/0/1: Other, IP, ARP, CDP
GigabitEthernet1/0/2: Other, IP
GigabitEthernet1/0/3: Other, IP
GigabitEthernet1/0/4: Other, IP
GigabitEthernet1/0/5: Other, IP
GigabitEthernet1/0/6: Other, IP
GigabitEthernet1/0/7: Other, IP
GigabitEthernet1/0/8: Other, IP
GigabitEthernet1/0/9: Other, IP
GigabitEthernet1/0/10: Other, IP, CDP

<output truncated>
```

This is an example of output from the **show interfaces counters trunk** command. It displays trunk counters for all interfaces.

```
Controller# show interfaces counters trunk
Port        TrunkFramesTx   TrunkFramesRx   WrongEncap
Gi1/0/1                 0               0            0
Gi1/0/2                 0               0            0
Gi1/0/3             80678               0            0
Gi1/0/4             82320               0            0
Gi1/0/5                 0               0            0

<output truncated>
```

show location

To display location information for an endpoint, use the **show location** command in EXEC mode.

show location admin-tag

show location civic-location identifier *string* **interface** *interface-id* **static**

show location elin-location identifier *string* **interface** *interface-id* **static**

Syntax Description

admin-tag	Displays administrative tag or site information.
civic-location	Displays civic location information.
elin-location	Displays emergency location information (ELIN).
identifier *string*	Specifies the ID for the civic location or the ELIN location. The range is 1 to 4095.
interface *interface-id*	Displays location information for the specified interface or all interfaces. Valid interfaces include physical ports.
static	Displays static configuration information.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This is an example of output from the **show location civic-location** command that displays location information for an interface:

```
Controller# show location civic-location interface gigabitethernet2/0/1
Civic location information
--------------------------
Identifier              : 1
County                  : Santa Clara
Street number           : 3550
Building                : 19
Room                    : C6
Primary road name       : Cisco Way
City                    : San Jose
State                   : CA
Country                 : US
```

This is an example of output from the **show location civic-location** command that displays all the civic location information:

```
Controller# show location civic-location static
Civic location information
---------------------------
Identifier              : 1
County                  : Santa Clara
Street number           : 3550
Building                : 19
Room                    : C6
Primary road name       : Cisco Way
City                    : San Jose
State                   : CA
Country                 : US
Ports                   : Gi2/0/1
---------------------------
Identifier              : 2
Street number           : 24568
Street number suffix    : West
Landmark                : Golden Gate Bridge
Primary road name       : 19th Ave
City                    : San Francisco
Country                 : US
---------------------------
```

This is an example of output from the **show location elin-location** command that displays the emergency location information:

```
Controller# show location elin-location identifier 1
Elin location information
---------------------------
Identifier : 1
Elin       : 14085553881
Ports      : Gi2/0/2
```

This is an example of output from the **show location elin-location static** command that displays all emergency location information:

```
Controller# show location elin-location static
Elin location information
---------------------------
Identifier : 1
Elin       : 14085553881
Ports      : Gi2/0/2
---------------------------
Identifier : 2
Elin       : 18002228999
---------------------------
```

show mgmt-infra trace messages ilpower-ha

To display inline power high availability messages within a trace buffer, use the **show mgmt-infra trace messages ilpower-ha** command in privileged EXEC mode.

show mgmt-infra trace messages ilpower-ha [**switch** *stack-member-number*]

Syntax Description

switch *stack-member-number*	(Optional) Specifies the stack member number for which to display inline power messages within a trace buffer.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This is an output example from the **show mgmt-infra trace messages ilpower-ha** command:

```
Controller# show mgmt-infra trace messages ilpower-ha
[10/23/12 14:04:48.087 UTC 1 3] NG3K_ILPOWER_HA: Created NGWC ILP CF client succ
essfully.
```

show network-policy profile

To display the network-policy profiles, use the **show network policy profile** command in privileged EXEC mode.

show network-policy profile [*profile-number*] [**detail**]

Syntax Description

profile-number	(Optional) Displays the network-policy profile number. If no profile is entered, all network-policy profiles appear.
detail	(Optional) Displays detailed status and statistics information.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This is an example of output from the **show network-policy profile** command:

```
Controller# show network-policy profile
Network Policy Profile 10
   voice vlan 17 cos 4
  Interface:
   none
Network Policy Profile 30
   voice vlan 30 cos 5
  Interface:
   none
Network Policy Profile 36
   voice vlan 4 cos 3
  Interface:
   Interface_id
```

show nmsp

To display the Network Mobility Services Protocol (NMSP) information for the switch, use the **show nmsp** command in privileged EXEC mode.

show nmsp {**attachment suppress interface**| **capability**| **notification interval**| **statistics** {**connection**| **summary**}| **status**| **subscription** {**detail**| **summary**}}

Syntax Description

attachment suppress interface	Displays attachment suppress interfaces.
capability	Displays switch capabilities including the supported services and subservices.
notification interval	Displays the notification intervals of the supported services.
statistics	Displays the NMSP statistics information.
connection	Displays the message counters on each connection.
summary	Displays the global counters.
status	Displays information about the NMSP connections.
subscription	Displays the subscription information on each NMSP connection.
detail	Displays all services and subservices subscribed on each connection.
summary	Displays all services subscribed on each connection.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This is an example of output from the **show nmsp attachment suppress interface** command:

```
Controller# show nmsp attachment suppress interface
NMSP Attachment Suppression Interfaces
------------------------------------
GigabitEthernet1/0/1
```

```
GigabitEthernet1/0/3
```

This is an example of output from the **show nmsp capability** command:

```
Controller# show nmsp capability
Service         Subservice
-------------------------
RSSI            Mobile Station, Tags, Rogue
Info            Mobile Station, Rogue
Statistics      Mobile Station, Tags
Attachment      Wired Station
Location        Subscription
AP Monitor      Subscription
IDS Services    WIPS
```

This is an example of output from the **show nmsp notification interval** command:

```
Controller# show nmsp notification interval
NMSP Notification Intervals
---------------------------

RSSI Interval:
  Client              : 2 sec
  RFID                : 2 sec
  Rogue AP            : 2 sec
  Rogue Client        : 2 sec
Attachment Interval   : 30 sec
Location Interval     : 30 sec
```

This is an example of output from the **show nmsp statistics summary** command:

```
Controller# show nmsp statistics summary
NMSP Global Counters
--------------------

Client measure send fail                   : 0
Send RSSI with no entry                    : 0
Application message too big                : 0
Failed select on accept socket             : 0
Failed SSL write                           : 0
Partial SSL write                          : 0
SSL write returned zero                    : 0
SSL write attempts to want read            : 0
SSL write attempts to want write           : 0
SSL write got default error                : 0
SSL write max data length sent             : 0
SSL write max attempts to write in loop    : 0
SSL read returned zero                     : 0
SSL read attempts to want read             : 0
SSL read attempts to want write            : 0
SSL read got default error                 : 0
Failed SSL read - con rx buf freed         : 0
Failed SSL read - con/SSL freed            : 0
Max records read before exiting SSL read   : 0
Highest priority tx queue full             : 0
Normal priority tx queue full              : 0
Highest priority tx queue count            : 0
Normal priority tx queue count             : 0
APP sent message to highest priority queue : 0
Max measure notify message                 : 0
Max info notify message                    : 0
Max highest priority tx queue count        : 0
Max normal priority tx queue count         : 0
Max receive queue count                    : 3
Max info notify queue count                : 0
Max client info notify delay               : 0
Max rogue AP info notify delay             : 0
Max rogue client info notify delay         : 0
Max client measure notify delay            : 0
Max tag measure notify delay               : 0
Max rogue AP measure notify delay          : 0
Max rogue client measure notify delay      : 0
Max client stats notify delay              : 0
```

```
Max RFID stats notify delay               : 0
RFID measurement periodic                 : 0
RFID measurement immediate                : 0
SSL handshake failed                      : 0
NMSP rx detected connection failure       : 0
NMSP tx detected connection failure       : 0
NMSP tx buf size exceeded                 : 0
Reconnect before connection Timeout       : 0
```

show platform CAPWAP summary

To display the tunnel identifier and the type all the CAPWAP tunnels established by the controller to the access points and other mobility controllers, use the **show platform CAPWAP summary** command.

show platform CAPWAP summary

Syntax Description

This command has no keywords or arguments.

Command Default

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example displays the tunnel identifier and details:

```
Controller# show platform capwap summary
Tunnel ID | Type | Src IP | Dst IP | SPrt | DPrt | S | A
------------------------------------------------------------------------------

0x0088498000000983 data 9.6.44.61 9.12.138.101 5247 41894 1 1

0x00966dc000000010 data 9.6.44.61 9.6.47.101 5247 62526 1 2
0x00938e800000095b data 9.6.44.61 9.12.138.100 5247 45697 1 1

0x00ab1a8000000bd1 data 9.6.44.61 9.12.139.101 5247 38906 1 0

0x00896e40000000bd data 9.6.44.61 9.12.136.100 5247 1836 1 1
```

show network-policy profile

To display the network-policy profiles, use the **show network policy profile** command in privileged EXEC mode.

show network-policy profile [*profile-number*] [**detail**]

Syntax Description

profile-number	(Optional) Displays the network-policy profile number. If no profile is entered, all network-policy profiles appear.
detail	(Optional) Displays detailed status and statistics information.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This is an example of output from the **show network-policy profile** command:

```
Controller# show network-policy profile
Network Policy Profile 10
   voice vlan 17 cos 4
  Interface:
   none
Network Policy Profile 30
   voice vlan 30 cos 5
  Interface:
   none
Network Policy Profile 36
   voice vlan 4 cos 3
  Interface:
   Interface_id
```

show wireless interface summary

To display the wireless interface status and configuration, use the **show wireless interface summary** command.

The command displays the total number of packets that are sent or received by the controllers.

show wireless interface summary

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to display the summary of wireless interfaces.

```
Controller# show wireless interface summary

Interface Name Interface Type VLAN ID IP Address IP Netmask MAC Address
-----------------------------------------------------------------------------

Vlan10 Management 10 10.5.1.11 255.255.255.0   2037.0652.72c6
```

system mtu

Syntax Description

bytes

Command Default

The default MTU size for all ports is 1500 bytes.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You can verify your setting by entering the **show system mtu** privileged EXEC command.

The switch does not support the MTU on a per-interface basis.

If you enter a value that is outside the allowed range for the specific type of interface, the value is not accepted.

voice-signaling vlan (network-policy configuration)

To create a network-policy profile for the voice-signaling application type, use the **voice-signaling vlan** command in network-policy configuration mode. To delete the policy, use the **no** form of this command.

voice-signaling vlan {*vlan-id* [**cos** *cos-value*| **dscp** *dscp-value*]| **dot1p** [**cos** *l2-priority*| **dscp** *dscp*]| **none**| **untagged**}

Syntax Description

vlan-id	(Optional) The VLAN for voice traffic. The range is 1 to 4094.
cos *cos-value*	(Optional) Specifies the Layer 2 priority class of service (CoS) for the configured VLAN. The range is 0 to 7; the default is 5.
dscp *dscp-value*	(Optional) Specifies the differentiated services code point (DSCP) value for the configured VLAN. The range is 0 to 63; the default is 46.
dot1p	(Optional) Configures the phone to use IEEE 802.1p priority tagging and to use VLAN 0 (the native VLAN).
none	(Optional) Does not instruct the Cisco IP phone about the voice VLAN. The phone uses the configuration from the phone key pad.
untagged	(Optional) Configures the phone to send untagged voice traffic. This is the default for the phone.

Command Default

No network-policy profiles for the voice-signaling application type are defined.

The default CoS value is 5.

The default DSCP value is 46.

The default tagging mode is untagged.

Command Modes

Network-policy profile configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Use the **network-policy profile** global configuration command to create a profile and to enter network-policy profile configuration mode.

The voice-signaling application type is for network topologies that require a different policy for voice signaling than for voice media. This application type should not be advertised if all of the same network policies apply as those advertised in the voice policy TLV.

When you are in network-policy profile configuration mode, you can create the profile for voice-signaling by specifying the values for VLAN, class of service (CoS), differentiated services code point (DSCP), and tagging mode.

These profile attributes are contained in the Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED) network-policy time-length-value (TLV).

To return to privileged EXEC mode from the network-policy profile configuration mode, enter the **exit** command.

Examples

This example shows how to configure voice-signaling for VLAN 200 with a priority 2 CoS:

```
Controller(config)# network-policy profile 1
Controller(config-network-policy)# voice-signaling vlan 200 cos 2
```

This example shows how to configure voice-signaling for VLAN 400 with a DSCP value of 45:

```
Controller(config)# network-policy profile 1
Controller(config-network-policy)# voice-signaling vlan 400 dscp 45
```

This example shows how to configure voice-signaling for the native VLAN with priority tagging:

```
Controller(config-network-policy)# voice-signaling vlan dot1p cos 4
```

voice vlan (network-policy configuration)

To create a network-policy profile for the voice application type, use the **voice vlan** command in network-policy configuration mode. To delete the policy, use the **no** form of this command.

voice vlan {*vlan-id* [**cos** *cos-value*| **dscp** *dscp-value*]| **dot1p** [**cos** *l2-priority*| **dscp** *dscp*]| **none**| **untagged**}

Syntax Description

vlan-id	(Optional) The VLAN for voice traffic. The range is 1 to 4094.
cos *cos-value*	(Optional) Specifies the Layer 2 priority class of service (CoS) for the configured VLAN. The range is 0 to 7; the default is 5.
dscp *dscp-value*	(Optional) Specifies the differentiated services code point (DSCP) value for the configured VLAN. The range is 0 to 63; the default is 46.
dot1p	(Optional) Configures the phone to use IEEE 802.1p priority tagging and to use VLAN 0 (the native VLAN).
none	(Optional) Does not instruct the Cisco IP phone about the voice VLAN. The phone uses the configuration from the phone key pad.
untagged	(Optional) Configures the phone to send untagged voice traffic. This is the default for the phone.

Command Default

No network-policy profiles for the voice application type are defined.

The default CoS value is 5.

The default DSCP value is 46.

The default tagging mode is untagged.

Command Modes

Network-policy profile configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Use the **network-policy profile** global configuration command to create a profile and to enter network-policy profile configuration mode.

The voice application type is for dedicated IP telephones and similar devices that support interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security through isolation from data applications.

When you are in network-policy profile configuration mode, you can create the profile for voice by specifying the values for VLAN, class of service (CoS), differentiated services code point (DSCP), and tagging mode.

These profile attributes are contained in the Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED) network-policy time-length-value (TLV).

To return to privileged EXEC mode from the network-policy profile configuration mode, enter the **exit** command.

Examples

This example shows how to configure the voice application type for VLAN 100 with a priority 4 CoS:

```
Controller(config)# network-policy profile 1
Controller(config-network-policy)# voice vlan 100 cos 4
```

This example shows how to configure the voice application type for VLAN 100 with a DSCP value of 34:

```
Controller(config)# network-policy profile 1
Controller(config-network-policy)# voice vlan 100 dscp 34
```

This example shows how to configure the voice application type for the native VLAN with priority tagging:

```
Controller(config-network-policy)# voice vlan dot1p cos 4
```

wireless ap-manager interface

To configure the wireless AP-manager interface, use the **wireless ap-manager interface** command.

wireless ap-managerinterface {**TenGigabitEthernet** *interface-number*| **Vlan** *interface-number*}

Syntax Description

TenGigabitEthernet *interface-name*	Configures 10-Gigabit Ethernet interface. Values range from 0 to 9.
Vlan *interface-name*	Configures VLANs. Values range from 1 to 4095.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to configure the wireless AP-manager:

```
Controller# wireless ap-manager interface vlan
<1-4095>  Vlan interface number
```

This example shows how to configure the wireless AP-manager:

```
Controller# #wireless ap-manager interface vlan 10
```

wireless exclusionlist

To manage exclusion list entries, use the **wireless exclusionlist** global configuration command. To remove the exclusion list entries, use the **no** form of the command.

wireless exclusionlist *mac-addr* **description** *description*

no wireless exclusionlist *mac-addr*

Syntax Description

mac-addr	The MAC address of the local excluded entry.
description *description*	Specifies the description for an exclusion-list entry.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to create a local exclusion list entry for the MAC address xxx.xxx.xxx:

```
Controller# wireless exclusionlist xxx.xxx.xxx
```

This example shows how to create a description for the local exclusion list entry for the MAC address xxx.xxx.xxx:

```
Controller# wireless exclusionlist xxx.xxx.xxx description sample
```

wireless linktest

To configure linktest frame size and number of frames to send, use the **wireless linktest** command.

wireless linktest {**frame-size** *size*| **number-of-frames** *value*}

Syntax Description

frame-size *size*	Specifies the link test frame size for each packet. The values range from 1 to 1400.
number-of-frames *value*	Specifies the number of frames to be sent for the link test. The values range from 1 to 100.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to configure the link test frame size of each frame as 10:

```
Controller# wireless linktest frame-size 10
```

wireless management interface

To configure wireless management parameters on an interface, use the **wireless management interface** global configuration command. To remove a wireless management parameters on an interface, use the **no** form of the command.

wireless management interface *interface-name* {**TenGigabitEthernet** *interface-name*| **Vlan** *interface-name*}

no wireless management interface

Syntax Description

interface-name	The interface number.
TenGigabitEthernet *interface-name*	The 10-Gigabit Ethernet interface number. The values range from 0 to 9.
Vlan *interface-name*	The VLAN interface number. The values range from 1 to 4095.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to configure VLAN 10 on the wireless interface:

```
Controller# wireless management interface Vlan 10
```

wireless peer-blocking forward-upstream

To configure peer-to-peer blocking for forward upstream, use the **wireless peer-blocking forward-upstream** command. To remove a peer-to-peer blocking, use the **no** form of the command.

wireless peer-blocking forward-upstream *interface*{**GigabitEthernet** *interface-number* **TenGigabitEthernet** *interface-number*}

no wireless peer-blocking forward-upstream {**GigabitEthernet** *interface-number* **TenGigabitEthernet** *interface-number*}

Syntax Description

GigabitEthernet *interface*	The Gigabit Ethernet interface number. Values range from 0 to 9.
TenGigabitEthernet *interface*	The 10-Gigabit Ethernet interface number. Values range from 0 to 9.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to configure peer-to-peer blocking for interface 10-gigabit ethernet interface:

```
Controller(config)# wireless peer-blocking forward-upstream TenGigabitEthernet 1/1/4
```

PART IV

VLAN

VLAN Commands

clear vmps statistics

To clear the VLAN Membership Policy Server (VMPS) statistics maintained by the VLAN Query Protocol (VQP) client, use the **clear vmps statistics** command in privileged EXEC mode.

clear vmps statistics

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You can verify that information was deleted by entering the **show vmps statistics** privileged EXEC command.

Examples

This example shows how to clear VLAN Membership Policy Server (VMPS) statistics:

```
Controller# clear vmps statistics
```

clear vtp counters

To clear the VLAN Trunking Protocol (VTP) and pruning counters, use the **clear vtp counters** command in privileged EXEC mode on the switch stack or on a standalone switch.

clear vtp counters

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to clear the VTP counters:

```
Controller# clear vtp counters
```

You can verify that information was deleted by entering the **show vtp counters** privileged EXEC command.

Related Commands

Command	Description
show vtp	Displays general information about VTP management domain, status, and counters.

debug sw-vlan

To enable debugging of VLAN manager activities, use the **debug sw-vlan** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug sw-vlan {**badpmcookies**| **cfg-vlan** {**bootup**| **cli**}| **events**| **ifs**| **mapping**| **notification**| **packets**| **redundancy**| **registries**| **vtp**}

no debug sw-vlan {**badpmcookies**| **cfg-vlan** {**bootup**| **cli**}| **events**| **ifs**| **mapping**| **notification**| **packets**| **redundancy**| **registries**| **vtp**}

Syntax Description

badpmcookies	Displays debug messages for VLAN manager incidents of bad port manager cookies.
cfg-vlan	Displays VLAN configuration debug messages.
bootup	Displays messages when the switch is booting up.
cli	Displays messages when the command-line interface (CLI) is in VLAN configuration mode.
events	Displays debug messages for VLAN manager events.
ifs	Displays debug messages for the VLAN manager IOS file system (IFS). See debug sw-vlan ifs, on page 264 for more information.
mapping	Displays debug messages for VLAN mapping.
packets	Displays debug messages for packet handling and encapsulation processes.
redundancy	Displays debug messages for VTP VLAN redundancy.
registries	Displays debug messages for VLAN manager registries.
vtp	Displays debug messages for the VLAN Trunking Protocol (VTP) code. See debug sw-vlan vtp, on page 267 for more information.

Command Default

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The **undebug sw-vlan** command is the same as the **no debug sw-vlan** command.

When you enable debugging on a switch stack, it is enabled only on the . To enable debugging on a stack member, start a session from the using the **session** *switch-number* EXEC command. Then enter the **debug** command at the command-line prompt of the stack member.

Related Commands

Command	Description
debug sw-vlan ifs	Enables debugging of the VLAN manager IOS file system (IFS) error tests.
debug sw-vlan notification	Enables debugging of the activation and deactivation of ISL VLAN IDs.
debug sw-vlan vtp	Enables debugging of the VTP code.
show vlan	Displays the parameters for all configured VLANs or one VLAN (if the VLAN ID or name is specified) in the administrative domain.
show vtp	Displays general information about VTP management domain, status, and counters.

debug sw-vlan ifs

To enable debugging of the VLAN manager IOS file system (IFS) error tests, use the **debug sw-vlan ifs** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug sw-vlan ifs {**open** {**read**| **write**}| **read** {**1**| **2**| **3**| **4**}| **write**}

no debug sw-vlan ifs {**open** {**read**| **write**}| **read** {**1**| **2**| **3**| **4**}| **write**}

Syntax Description

open read	Displays VLAN manager IFS file-read operation debug messages.
open write	Displays VLAN manager IFS file-write operation debug messages.
read	Displays file-read operation debug messages for the specified error test (1, 2, 3, or 4).
write	Displays file-write operation debug messages.

Command Default

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The **undebug sw-vlan ifs** command is the same as the **no debug sw-vlan ifs** command.

When you enable debugging on a switch stack, it is enabled only on the . To enable debugging on a stack member, start a session from the using the **session** *switch-number* EXEC command. Then enter the **debug** command at the command-line prompt of the stack member.

When selecting the file read operation, Operation **1** reads the file header, which contains the header verification word and the file version number. Operation **2** reads the main body of the file, which contains most of the domain and VLAN information. Operation **3** reads type length version (TLV) descriptor structures. Operation **4** reads TLV data.

Related Commands

Command	Description
show vlan	Displays the parameters for all configured VLANs or one VLAN (if the VLAN ID or name is specified) in the administrative domain.

debug sw-vlan notification

To enable debugging of the activation and deactivation of Inter-Link Switch (ISL) VLAN IDs, use the **debug sw-vlan notification** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug sw-vlan notification {**accfwdchange| allowedvlancfgchange| fwdchange| linkchange| modechange| pruningcfgchange| statechange**}

no debug sw-vlan notification {**accfwdchange| allowedvlancfgchange| fwdchange| linkchange| modechange| pruningcfgchange| statechange**}

Syntax Description

accfwdchange	Displays debug messages for VLAN manager notification of aggregated access interface spanning-tree forward changes.
allowedvlancfgchange	Displays debug messages for VLAN manager notification of changes to the allowed VLAN configuration.
fwdchange	Displays debug messages for VLAN manager notification of spanning-tree forwarding changes.
linkchange	Displays debug messages for VLAN manager notification of interface link-state changes.
modechange	Displays debug messages for VLAN manager notification of interface mode changes.
pruningcfgchange	Displays debug messages for VLAN manager notification of changes to the pruning configuration.
statechange	Displays debug messages for VLAN manager notification of interface state changes.

Command Default

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The **undebug sw-vlan notification** command is the same as the **no debug sw-vlan notification** command.

When you enable debugging on a switch stack, it is enabled only on the . To enable debugging on a stack member, start a session from the using the **session** *switch-number* EXEC command. Then enter the **debug** command at the command-line prompt of the stack member.

Related Commands

Command	Description
show vlan	Displays the parameters for all configured VLANs or one VLAN (if the VLAN ID or name is specified) in the administrative domain.

debug sw-vlan vtp

To enable debugging of the VLAN Trunking Protocol (VTP) code, use the **debug sw-vlan vtp** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug sw-vlan vtp {**events**| **packets**| **pruning** [**packets**| **xmit**]| **redundancy**| **xmit**}

no debug sw-vlan vtp {**events**| **packets**| **pruning**| **redundancy**| **xmit**}

Syntax Description

events	Displays debug messages for general-purpose logic flow and detailed VTP messages generated by the VTP_LOG_RUNTIME macro in the VTP code.
packets	Displays debug messages for the contents of all incoming VTP packets that have been passed into the VTP code from the Cisco IOS VTP platform-dependent layer, except for pruning packets.
pruning	Displays debug messages generated by the pruning segment of the VTP code.
packets	(Optional) Displays debug messages for the contents of all incoming VTP pruning packets that have been passed into the VTP code from the Cisco IOS VTP platform-dependent layer.
xmit	(Optional) Displays debug messages for the contents of all outgoing VTP packets that the VTP code requests the Cisco IOS VTP platform-dependent layer to send.
redundancy	Displays debug messages for VTP redundancy.
xmit	Displays debug messages for the contents of all outgoing VTP packets that the VTP code requests the Cisco IOS VTP platform-dependent layer to send, except for pruning packets.

Command Default

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The **undebug sw-vlan vtp** command is the same as the **no debug sw-vlan vtp** command.

When you enable debugging on a switch stack, it is enabled only on the . To enable debugging on a stack member, start a session from the using the **session** *switch-number* EXEC command. Then enter the **debug** command at the command-line prompt of the stack member.

If no further parameters are entered after the **pruning** keyword, VTP pruning debugging messages appear. They are generated by the VTP_PRUNING_LOG_NOTICE, VTP_PRUNING_LOG_INFO, VTP_PRUNING_LOG_DEBUG, VTP_PRUNING_LOG_ALERT, and VTP_PRUNING_LOG_WARNING macros in the VTP pruning code.

Related Commands

Command	Description
show vtp	Displays general information about VTP management domain, status, and counters.

interface vlan

To create or access a dynamic switch virtual interface (SVI) and to enter interface configuration mode, use the **interface vlan** command in global configuration mode. To delete an SVI, use the **no** form of this command.

interface vlan *vlan-id*

no interface vlan *vlan-id*

Syntax Description

vlan-id	VLAN number. The range is 1 to 4094.

Command Default

The default VLAN interface is VLAN 1.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

SVIs are created the first time you enter the **interface vlan** *vlan-id* command for a particular VLAN. The *vlan-id* corresponds to the VLAN-tag associated with data frames on an IEEE 802.1Q encapsulated trunk or the VLAN ID configured for an access port.

Note When you create an SVI, it does not become active until it is associated with a physical port.

If you delete an SVI using the **no interface vlan** *vlan-id* command, it is no longer visible in the output from the **show interfaces** privileged EXEC command.

Note You cannot delete the VLAN 1 interface.

You can re-instate a deleted SVI by entering the **interface vlan** *vlan-id* command for the deleted interface. The interface comes back up, but the previous configuration is gone.

The interrelationship between the number of SVIs configured on a switch or a switch stack and the number of other features being configured might have an impact on CPU utilization due to hardware limitations. You can use the **sdm prefer** global configuration command to reallocate system hardware resources based on templates and feature tables.

You can verify your setting by entering the **show interfaces** and **show interfaces vlan** *vlan-id* privileged EXEC commands.

Examples

This example shows how to create a new SVI with VLAN ID 23 and enter interface configuration mode:

```
Controller(config)# interface vlan 23
Controller(config-if)#
```

Related Commands

Command	Description
show interfaces	Displays the administrative and operational status of all interfaces or a specified interface.

remote-span

To configure a VLAN as a Remote Switched Port Analyzer (RSPAN) VLAN, use the **remote-span** command in VLAN configuration mode on the switch stack or on a standalone switch. To remove the RSPAN designation from the VLAN, use the **no** form of this command.

remote-span

no remote-span

Syntax Description

This command has no keywords or arguments.

Command Default

No RSPAN VLANs are defined.

Command Modes

VLAN configuration (config-VLAN)

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

If VLAN Trunking Protocol (VTP) is enabled, the RSPAN feature is propagated by VTP for VLAN IDs that are lower than 1005. If the RSPAN VLAN ID is in the extended range, you must manually configure intermediate switches (those in the RSPAN VLAN between the source switch and the destination switch).

Before you configure the RSPAN **remote-span** command, use the **vlan** (global configuration) command to create the VLAN.

The RSPAN VLAN has these characteristics:

- No MAC address learning occurs on it.
- RSPAN VLAN traffic flows only on trunk ports.
- Spanning Tree Protocol (STP) can run in the RSPAN VLAN, but it does not run on RSPAN destination ports.

When an existing VLAN is configured as an RSPAN VLAN, the VLAN is first deleted and then recreated as an RSPAN VLAN. Any access ports are made inactive until the RSPAN feature is disabled.

Examples

This example shows how to configure a VLAN as an RSPAN VLAN:

```
Controller(config)# vlan 901
Controller(config-vlan)# remote-span
```

This example shows how to remove the RSPAN feature from a VLAN:

```
Controller(config)# vlan 901
Controller(config-vlan)# no remote-span
```

You can verify your settings by entering the **show vlan remote-span** user EXEC command.

Related Commands

Command	Description
monitor session destination	Configures a FSPAN or FRSPAN destination session.
monitor session filter	Configures a FSPAN or FRSPAN session filter.
monitor session source	Configures a FSPAN or FRSPAN source session.
show vlan	Displays the parameters for all configured VLANs or one VLAN (if the VLAN ID or name is specified) in the administrative domain.
vlan	Adds a VLAN and enters the VLAN configuration mode.

show vlan

To display the parameters for all configured VLANs or one VLAN (if the VLAN ID or name is specified) on the switch, use the **show vlan** command in user EXEC mode.

show vlan [**brief**| **id** *vlan-id*| **mtu**| **name** *vlan-name*| **remote-span**| **summary**]

Syntax Description

brief	(Optional) Displays one line for each VLAN with the VLAN name, status, and its ports.
id *vlan-id*	(Optional) Displays information about a single VLAN identified by the VLAN ID number. For *vlan-id*, the range is 1 to 4094.
mtu	(Optional) Displays a list of VLANs and the minimum and maximum transmission unit (MTU) sizes configured on ports in the VLAN.
name *vlan-name*	(Optional) Displays information about a single VLAN identified by the VLAN name. The VLAN name is an ASCII string from 1 to 32 characters.
remote-span	(Optional) Displays information about Remote SPAN (RSPAN) VLANs.
summary	(Optional) Displays VLAN summary information.

Note Though visible in the command-line help string, the **ifindex** keyword is not supported.

Command Default

None

Command Modes

User EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

In the **show vlan mtu** command output, the MTU_Mismatch column shows whether all the ports in the VLAN have the same MTU. When yes appears in the column, it means that the VLAN has ports with different MTUs, and packets that are switched from a port with a larger MTU to a port with a smaller MTU might be dropped. If the VLAN does not have an SVI, the hyphen (-) symbol appears in the SVI_MTU column. If the MTU-Mismatch column displays yes, the names of the ports with the MinMTU and the MaxMTU appear.

Examples

This is an example of output from the **show vlan** command. See the table that follows for descriptions of the fields in the display.

Table 7: show vlan Command Output Fields

Field	Description
VLAN	VLAN number.
Name	Name, if configured, of the VLAN.
Status	Status of the VLAN (active or suspend).
Ports	Ports that belong to the VLAN.
Type	Media type of the VLAN.
SAID	Security association ID value for the VLAN.
MTU	Maximum transmission unit size for the VLAN.
Parent	Parent VLAN, if one exists.
RingNo	Ring number for the VLAN, if applicable.
BrdgNo	Bridge number for the VLAN, if applicable.
Stp	Spanning Tree Protocol type used on the VLAN.
BrdgMode	Bridging mode for this VLAN—possible values are source-route bridging (SRB) and source-route transparent (SRT); the default is SRB.
Trans1	Translation bridge 1.
Trans2	Translation bridge 2.
Remote SPAN VLANs	Identifies any RSPAN VLANs that have been configured.

This is an example of output from the **show vlan summary** command:

```
Controller> show vlan summary
Number of existing VLANs              : 45
 Number of existing VTP VLANs         : 45
 Number of existing extended VLANS    : 0
```

This is an example of output from the **show vlan id** command:

```
Controller# show vlan id 2
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
2    VLAN0200                         active    Gi1/0/7, Gi1/0/8
2    VLAN0200                         active    Gi2/0/1, Gi2/0/2
```

```
VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
2    enet  100002     1500  -      -      -        -    -        0      0

Remote SPAN VLANs
------------------------------------------------------------------------------
Disabled
```

Related Commands

Command	Description
switchport mode	Configures the VLAN membership mode of a port.
vlan	Adds a VLAN and enters the VLAN configuration mode.

show vlan filter

To display information about all VLAN filters or about a particular VLAN or VLAN access map, use the **show vlan filter** command in privileged EXEC mode.

show vlan filter {**access-map** *name*| **vlan** *vlan-id*}

Syntax Description

access-map *name*	(Optional) Displays filtering information for the specified VLAN access map.
vlan *vlan-id*	(Optional) Displays filtering information for the specified VLAN. The range is 1 to 4094.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This is an example of output from the **show vlan filter** command:

```
Controller# show vlan filter
VLAN Map map_1 is filtering VLANs:
  20-22
```

Related Commands

Command	Description
show vlan access-map	Displays the VLAN access maps created on the switch.
vlan access-map	Defines a VLAN map and enters access-map configuration mode where you can specify a MAC ACL to match and the action to be taken.
vlan filter	Applies a VLAN map to one or more VLANs.

show vlan group

To display the VLANs that are mapped to VLAN groups, use the **show vlan group** command in privileged EXEC mode.

show vlan group [**group-name** *vlan-group-name* **[user_count]**]

Syntax Description

group-name *vlan-group-name*	(Optional) Displays the VLANs mapped to the specified VLAN group.
user_count	(Optional) Displays the number of users in each VLAN mapped to a specified VLAN group.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The **show vlan group** command displays the existing VLAN groups and lists the VLANs and VLAN ranges that are members of each VLAN group. If you enter the **group-name** keyword, only the members of the specified VLAN group are displayed.

Examples

This example shows how to display the members of a specified VLAN group:

This example shows how to display number of users in each of the VLANs in a group:

```
Controller# show vlan group group-name group2 user_count
  VLAN     : Count
--------------------
  40         : 5
  41         : 8
  42         : 12
  43         : 2
  44         : 9
  45         : 0
```

Related Commands

Command	Description
vlan group	Creates or modifies a VLAN group.

show vtp

To display general information about the VLAN Trunking Protocol (VTP) management domain, status, and counters, use the **show vtp** command in EXEC mode.

show vtp {**counters**| **devices** [**conflicts**]| **interface** [*interface-id*]| **password**| **status**}

Syntax Description

counters	Displays the VTP statistics for the switch.
devices	Displays information about all VTP version 3 devices in the domain. This keyword applies only if the switch is not running VTP version 3.
conflicts	(Optional) Displays information about VTP version 3 devices that have conflicting primary servers. This command is ignored when the switch is in VTP transparent or VTP off mode.
interface	Displays VTP status and configuration for all interfaces or the specified interface.
interface-id	(Optional) Interface for which to display VTP status and configuration. This can be a physical interface or a port channel.
password	Displays the configured VTP password (available in privileged EXEC mode only).
status	Displays general information about the VTP management domain status.

Command Default

None

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

When you enter the **show vtp password** command when the switch is running VTP version 3, the display follows these rules:

- If the **password** *password* global configuration command did not specify the **hidden** keyword and encryption is not enabled on the switch, the password appears in clear text.

- If the **password** *password* command did not specify the **hidden** keyword and encryption is enabled on the switch, the encrypted password appears.
- If the **password** *password* command is included the **hidden** keyword, the hexadecimal secret key is displayed.

Examples

This is an example of output from the **show vtp devices** command. A Yes in the Conflict column means that the responding server is in conflict with the local server for the feature; that is, when two switches in the same domain do not have the same primary server for a database.

```
Controller# show vtp devices
Retrieving information from the VTP domain. Waiting for 5 seconds.
VTP Database Conf switch ID      Primary Server Revision   System Name
             lict
------------ ---- --------------- -------------- ---------- ----------------------
VLAN         Yes  00b0.8e50.d000 000c.0412.6300 12354      main.cisco.com
MST          No   00b0.8e50.d000 0004.AB45.6000 24         main.cisco.com
VLAN         Yes  000c.0412.6300=000c.0412.6300 67         qwerty.cisco.com
```

This is an example of output from the **show vtp counters** command. The table that follows describes each field in the display.

```
Controller> show vtp counters
VTP statistics:
Summary advertisements received    : 0
Subset advertisements received     : 0
Request advertisements received    : 0
Summary advertisements transmitted : 0
Subset advertisements transmitted  : 0
Request advertisements transmitted : 0
Number of config revision errors   : 0
Number of config digest errors     : 0
Number of V1 summary errors        : 0

VTP pruning statistics:

Trunk            Join Transmitted Join Received    Summary advts received from
                                                   non-pruning-capable device
---------------- ---------------- ---------------- ---------------------------
Gi1/0/47              0                0                0
Gi1/0/48              0                0                0
Gi2/0/1               0                0                0
Gi3/0/2               0                0                0
```

Table 8: show vtp counters Field Descriptions

Field	Description
Summary advertisements received	Number of summary advertisements received by this switch on its trunk ports. Summary advertisements contain the management domain name, the configuration revision number, the update timestamp and identity, the authentication checksum, and the number of subset advertisements to follow.
Subset advertisements received	Number of subset advertisements received by this switch on its trunk ports. Subset advertisements contain all the information for one or more VLANs.

Field	Description
Request advertisements received	Number of advertisement requests received by this switch on its trunk ports. Advertisement requests normally request information on all VLANs. They can also request information on a subset of VLANs.
Summary advertisements transmitted	Number of summary advertisements sent by this switch on its trunk ports. Summary advertisements contain the management domain name, the configuration revision number, the update timestamp and identity, the authentication checksum, and the number of subset advertisements to follow.
Subset advertisements transmitted	Number of subset advertisements sent by this switch on its trunk ports. Subset advertisements contain all the information for one or more VLANs.
Request advertisements transmitted	Number of advertisement requests sent by this switch on its trunk ports. Advertisement requests normally request information on all VLANs. They can also request information on a subset of VLANs.
Number of configuration revision errors	Number of revision errors. Whenever you define a new VLAN, delete an existing one, suspend or resume an existing VLAN, or modify the parameters on an existing VLAN, the configuration revision number of the switch increments. Revision errors increment whenever the switch receives an advertisement whose revision number matches the revision number of the switch, but the MD5 digest values do not match. This error means that the VTP password in the two switches is different or that the switches have different configurations. These errors means that the switch is filtering incoming advertisements, which causes the VTP database to become unsynchronized across the network.

Field	Description
Number of configuration digest errors	Number of MD5 digest errors. Digest errors increment whenever the MD5 digest in the summary packet and the MD5 digest of the received advertisement calculated by the switch do not match. This error usually means that the VTP password in the two switches is different. To solve this problem, make sure the VTP password on all switches is the same. These errors mean that the switch is filtering incoming advertisements, which causes the VTP database to become unsynchronized across the network.
Number of V1 summary errors	Number of Version 1 errors. Version 1 summary errors increment whenever a switch in VTP V2 mode receives a VTP Version 1 frame. These errors mean that at least one neighboring switch is either running VTP Version 1 or VTP Version 2 with V2-mode disabled. To solve this problem, change the configuration of the switches in VTP V2-mode to disabled.
Join Transmitted	Number of VTP pruning messages sent on the trunk.
Join Received	Number of VTP pruning messages received on the trunk.
Summary Advts Received from non-pruning-capable device	Number of VTP summary messages received on the trunk from devices that do not support pruning.

This is an example of output from the **show vtp status** command. The table that follows describes each field in the display.

Table 9: show vtp status Field Descriptions

Field	Description
VTP Version capable	Displays the VTP versions that are capable of operating on the switch.
VTP Version running	Displays the VTP version operating on the switch. By default, the switch implements Version 1 but can be set to Version 2.
VTP Domain Name	Name that identifies the administrative domain for the switch.

Field	Description
VTP Pruning Mode	Displays whether pruning is enabled or disabled. Enabling pruning on a VTP server enables pruning for the entire management domain. Pruning restricts flooded traffic to those trunk links that the traffic must use to access the appropriate network devices.
VTP Traps Generation	Displays whether VTP traps are sent to a network management station.
Device ID	Displays the MAC address of the local device.
Configuration last modified	Displays the date and time of the last configuration modification. Displays the IP address of the switch that caused the configuration change to the database.
VTP Operating Mode	Displays the VTP operating mode, which can be server, client, or transparent. **Server—**A switch in VTP server mode is enabled for VTP and sends advertisements. You can configure VLANs on it. The switch guarantees that it can recover all the VLAN information in the current VTP database from NVRAM after reboot. By default, every switch is a VTP server. **Note** The switch automatically changes from VTP server mode to VTP client mode if it detects a failure while writing the configuration to NVRAM and cannot return to server mode until the NVRAM is functioning. **Client—**A switch in VTP client mode is enabled for VTP, can send advertisements, but does not have enough nonvolatile storage to store VLAN configurations. You cannot configure VLANs on it. When a VTP client starts up, it does not send VTP advertisements until it receives advertisements to initialize its VLAN database. **Transparent—**A switch in VTP transparent mode is disabled for VTP, does not send or learn from advertisements sent by other devices, and cannot affect VLAN configurations on other devices in the network. The switch receives VTP advertisements and forwards them on all trunk ports except the one on which the advertisement was received.
Maximum VLANs Supported Locally	Maximum number of VLANs supported locally.
Number of Existing VLANs	Number of existing VLANs.

Field	Description
Configuration Revision	Current configuration revision number on this switch.
MD5 Digest	A 16-byte checksum of the VTP configuration.

This is an example of output from the **show vtp status** command for a switch running VTP version 3:

```
Controller> show vtp status
VTP Version capable : 1 to 3
VTP version running : 3
VTP Domain Name : Cisco
VTP Pruning Mode : Disabled
VTP Traps Generation : Disabled
Device ID : 0021.1bcd.c700

Feature VLAN:
--------------
VTP Operating Mode : Server
Number of existing VLANs : 7
Number of existing extended VLANs : 0
Configuration Revision : 0
Primary ID : 0000.0000.0000
Primary Description :
MD5 digest : 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00

Feature MST:
--------------
VTP Operating Mode : Client
Configuration Revision : 0
Primary ID : 0000.0000.0000
Primary Description :
MD5 digest : 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00

Feature UNKNOWN:
----------------
```

Related Commands

Command	Description
clear vtp counters	Clears the VLAN Trunking Protocol (VTP) and pruning counters.

show wireless vlan group

To display the wireless VLAN group summary, use the **show wireless vlan group** command in privileged EXEC mode.

show wireless vlan group *group-name*

Syntax Description

group-name	Name of the wireless VLAN group.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

None

Examples

This example shows how to display the summary of a VLAN group:

```
Controller# show wireless vlan group grp1
```

spanning-tree vlan

To configure spanning tree on a per-VLAN basis, use the **spanning-tree vlan** command in global configuration mode on the switch stack or on a standalone switch. To return to the default setting, use the **no** form of this command.

spanning-tree vlan *vlan-id* [**forward-time** *seconds*| **hello-time** *seconds*| **max-age** *seconds*| **priority** *priority*| **root** {**primary**| **secondary**} [**diameter** *net-diameter* [**hello-time** *seconds*]]]

no spanning-tree vlan *vlan-id* [**forward-time**| **hello-time**| **max-age**| **priority**| **root**]

Syntax Description

vlan-id	VLAN range associated with a spanning-tree instance. You can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094.
forward-time *seconds*	(Optional) Sets the forward-delay time for the specified spanning-tree instance. The forwarding time specifies how long each of the listening and learning states last before the interface begins forwarding. The range is 4 to 30 seconds.
hello-time *seconds*	(Optional) Sets the interval between hello bridge protocol data units (BPDUs) sent by the root switch configuration messages. The range is 1 to 10 seconds.
max-age *seconds*	(Optional) Sets the interval between messages the spanning tree receives from the root switch. If a switch does not receive a BPDU message from the root switch within this interval, it recomputes the spanning-tree topology. The range is 6 to 40 seconds.
priority *priority*	(Optional) Sets the switch priority for the specified spanning-tree instance. This setting affects the likelihood that the switch is selected as the root switch. A lower value increases the probability that the switch is selected as the root switch. The range is 0 to 61440 in increments of 4096. Valid priority values are 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440. All other values are rejected.
root primary	(Optional) Forces this switch to be the root switch.
root secondary	(Optional) Sets this switch to be the root switch should the primary root switch fail.
diameter *net-diameter*	(Optional) Sets the maximum number of switches between any two end stations. The range is 2 to 7.

Command Default

Spanning tree is enabled on all VLANs.

The forward-delay time is 15 seconds.

The hello time is 2 seconds.

The max-age is 20 seconds.

The primary root switch priority is 24576.

The secondary root switch priority is 28672.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Disabling the STP causes the VLAN to stop participating in the spanning-tree topology. Interfaces that are administratively down remain down. Received BPDUs are forwarded like other multicast frames. The VLAN does not detect and prevent loops when STP is disabled.

You can disable the STP on a VLAN that is not currently active and verify the change by using the **show running-config** or the **show spanning-tree vlan** *vlan-id* privileged EXEC command. The setting takes effect when the VLAN is activated.

When disabling or reenabling the STP, you can specify a range of VLANs that you want to disable or enable.

When a VLAN is disabled and then enabled, all assigned VLANs continue to be its members. However, all spanning-tree bridge parameters are returned to their previous settings (the last setting before the VLAN was disabled).

You can enable spanning-tree options on a VLAN that has no interfaces assigned to it. The setting takes effect when you assign interfaces to it.

When setting the **max-age** *seconds*, if a switch does not receive BPDUs from the root switch within the specified interval, it recomputes the spanning-tree topology. The max-age setting must be greater than the hello-time setting.

The **spanning-tree vlan** *vlan-id* **root** command should be used only on backbone switches.

When you enter the **spanning-tree vlan** *vlan-id* **root** command, the software checks the switch priority of the current root switch for each VLAN. Because of the extended system ID support, the switch sets the switch priority for the specified VLAN to 24576 if this value will cause this switch to become the root for the specified VLAN. If any root switch for the specified VLAN has a switch priority lower than 24576, the switch sets its own priority for the specified VLAN to 4096 less than the lowest switch priority. (4096 is the value of the least-significant bit of a 4-bit switch priority value.)

When you enter the **spanning-tree vlan** *vlan-id* **root secondary** command, because of support for the extended system ID, the software changes the switch priority from the default value (32768) to 28672. If the root switch should fail, this switch becomes the next root switch (if the other switches in the network use the default switch priority of 32768, and therefore, are unlikely to become the root switch).

Examples

This example shows how to disable the STP on VLAN 5:

```
Controller(config)# no spanning-tree vlan 5
```

You can verify your setting by entering the **show spanning-tree** privileged EXEC command. In this instance, VLAN 5 does not appear in the list.

This example shows how to set the spanning-tree forwarding time to 18 seconds for VLANs 20 and 25:

```
Controller(config)# spanning-tree vlan 20,25 forward-time 18
```

This example shows how to set the spanning-tree hello-delay time to 3 seconds for VLANs 20 to 24:

```
Controller(config)# spanning-tree vlan 20-24 hello-time 3
```

This example shows how to set spanning-tree max-age to 30 seconds for VLAN 20:

```
Controller(config)# spanning-tree vlan 20 max-age 30
```

This example shows how to reset the max-age parameter to the default value for spanning-tree instance 100 and 105 to 108:

```
Controller(config)# no spanning-tree vlan 100, 105-108 max-age
```

This example shows how to set the spanning-tree priority to 8192 for VLAN 20:

```
Controller(config)# spanning-tree vlan 20 priority 8192
```

This example shows how to configure the switch as the root for VLAN 10 with a network diameter of 4:

```
Controller(config)# spanning-tree vlan 10 root primary diameter 4
```

This example shows how to configure the switch as the secondary root switch for VLAN 10 with a network diameter of 4:

```
Controller(config)# spanning-tree vlan 10 root secondary diameter 4
```

You can verify your settings by entering the **show spanning-tree vlan** *vlan-id* privileged EXEC command.

wireless broadcast vlan

To enable ethernet broadcast support on a VLAN, use the **wireless broadcast vlan** command in global configuration mode. To disable ethernet broadcast support, use the **no** form of the command.

wireless broadcast vlan [*vlan-id*]

no wireless broadcast vlan [*vlan-id*]

Syntax Description

vlan-id	(Optional) Specifies the VLAN ID to enable boradcast to that VLAN.

Command Default

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

None

Examples

This example shows how to enable broadcasting on VLAN 20:

```
Controller(config)# wireless broadcast vlan 20
```

wireless vlan group

To create a wireless VLAN group, use the **vlan group** command in interface configuration mode.

vlan group *group-name* **vlan-list** *vlan-id*

Syntax Description

group-name	Name of the VLAN group.
vlan-id	Range of the VLAN IDs to be added to the group.

Command Default

None

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The VLAN must be available to be grouped.

Examples

This example shows how to map VLANs 91 through 125 to a wireless VLAN group:

```
Controller(config)# wireless vlan group grp1 vlan-list 91-125
```

PART V

VideoStream

VideoStream Commands

ap dot11 mediastream

To configure various parameters, use the **ap dot11 mediastream** command.

ap dot11 {**24ghz**| **5ghz**} **media-stream** {**multicast-direct**| { **admission-besteffort**| *client-maximum value*}| **video-redirect**}

Syntax Description

multicast-direct	Configures multicast-direct.
admission-besteffort	Configures the media stream to still be sent through the best effort queue if a media stream cannot be prioritized due to bandwidth availability limitations.
client-maximum value	Configures maximum number of allowed media streams per individual client.
video-redirect	Configure to redirect unicast video to the Best Effort queue over the air.

Command Default

Disabled

Command Modes

config

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

None.

Examples

This example shows how to configure maximum number of allowed media streams per client.

```
Controller#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)#ap dot11 24ghz media-stream multicast-direct 15
```

ap dot11 media-stream multicast-direct

To configure multicast-direct for 2.4-GHz/5-GHz band, use the **ap dot11 media-stream multicast-direct** command.

ap dot11 {**24ghz**| **5ghz**} **media-stream** {**multicast-direct** {**admission-besteffort**| **client-maximum** *value*| **radio-maximum** *value*}| **video-redirect**}

Syntax Description

media-stream	Configure media-stream for 802.11 band.
multicast-direct	Configure multicast-direct for 802.11 band
admission-besteffort	Admits media stream to best-effort queue.
client-maximum *value*	Specifies the maximum number of streams allowed on a client.
radio-maximum *value*	Specifies the maximum number of streams allowed on a 2.4-GHz or a 5-GHz band.
video-redirect	Redirect non Multicast-direct video to BestEffort queue over the air.

Command Default

None.

Command Modes

config

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Before you configure the media stream multicast-direct parameters on a 802.11 network, ensure that the network is nonoperational.

Examples

This example shows how to configure multicast-direct for the 2.4-GHz band.

```
Controller#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)#ap dot11 24ghz media-stream multicast-direct admission-besteffort
```

show ap dot11

To display 802.11 band parameters, use the **show ap dot11** command.

show ap dot11 {**24ghz**| **5ghz**} {**media-stream rrc**| **network**| **profile**| **summary**}

Syntax Description

media-stream rrc	Display Media Stream configurations for 802.11b
network	802.11b network configuration.
profile	Shows 802.11b profiling information for all Cisco APs
summary	Shows configuration and statistics of 802.11b Cisco APs

Command Default

None.

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

None.

Examples

This example shows how to display 802.11 Media Resource Reservation Control configurations.

```
Controller#show ap dot11 24ghz media-stream rrc

Multicast-direct                : Disabled
Best Effort                     : Disabled
Video Re-Direct                 : Disabled
Max Allowed Streams Per Radio      : Auto
Max Allowed Streams Per Client     : Auto
Max Video Bandwidth              : 0
Max Voice Bandwidth              : 75
Max Media Bandwidth              : 85
Min PHY Rate (Kbps)              : 6000
Max Retry Percentage             : 80
```

show wireless media-stream group

To display the wireless media-stream group information, use the **show wireless media-stream group** command.

show wireless media-stream group {**detail** *groupName*| **summary**}

Syntax Description

detail *groupName*	Display media-stream group configuration details of the group mentioned in the command.
summary	Display media-stream group configuration summary

Command Default

None

Command Modes

Global config.

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

None.

Examples

This example shows how to display the details of the media-stream group named GRP1.

```
Controller#show wireless media-stream group detail GRP1
```

wireless media-stream multicast-direct

To configure multicast-direct status, use the **media-stream multicast-direct** command. To remove the multicast-direct status, use the no form of the command.

wireless media-stream multicast-direct

no wireless media-stream multicast-direct

Command Default

None.

Command Modes

wlan

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Media stream multicast-direct requires load based Call Admission Control (CAC) to run. WLAN quality of service (QoS) needs to be set to either gold or platinum.

Examples

This example shows how to configure multicast-direct for a wireless LAN media stream.

```
Controller#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)#wireless media-stream multicast-direct
```

wireless media-stream

To configure various parameters, use the **wireless media-stream** command.

wireless media-stream {**multicast-direct**| **message** [**phone** *phone*| **URL** *URL*| **Notes** *Notes*| **Email** *Email*]| **group** *groupName* [*startipAddr endipAddr*]}

Syntax Description

multicast-direct	Configure multicast-direct status.
message	Configure Session Announcement Message.
phone *phone*	Configure Session Announcement Phone number.
URL *URL*	Configure Session Announcement URL.
Notes *Notes*	Configure Session Announcement notes.
Email *Email*	Configure Session Announcement Email.
group *groupName*	Configure multicast-direct status for a group.
startipAddr	Specifies the start IP Address for the group.
endipAddr	Specifies the End IP Address for the group.

Command Default

Disabled

Command Modes

config

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Media-stream multicast-direct requires load-based Call Admission Control (CAC) to run.

Examples

This example shows how to configure each media stream and its parameters like expected multicast destination addresses, stream bandwidth consumption and stream priority parameters.

```
Controller#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)#wireless media-stream group GROUP1 231.1.1.1 231.1.1.10
```

PART VI

Multicast

IP Multicast Commands

This chapter contains IP Multicast commands that are relevant to the Catalyst 3850 switch.

ip igmp filter

Use the **ip igmp filter** interface configuration command on the controller stack or on a standalone controller to control whether or not all hosts on a Layer 2 interface can join one or more IP multicast groups by applying an Internet Group Management Protocol (IGMP) profile to the interface. Use the no form of this command to remove the specified profile from the interface.

ip igmp filter *profile number*

no ip igmp filter

Syntax Description

profile number	The IGMP profile number to be applied. The range is 1 to 4294967295.

Command Default

No IGMP filters are applied.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You can apply IGMP filters only to Layer 2 physical interfaces; you cannot apply IGMP filters to routed ports, switch virtual interfaces (SVIs), or ports that belong to an EtherChannel group.

An IGMP profile can be applied to one or more controller port interfaces, but one port can have only one profile applied to it.

Examples

This example shows how to configure IGMP profile 40 to permit the specified range of IP multicast addresses, then shows how to apply that profile to a port as a filter:

```
Controller(config)# ip igmp profile 40
Controller(config-igmp-profile)# permit
Controller(config-igmp-profile)# range 233.1.1.1 233.255.255.255
Controller(config-igmp-profile)# exit
Controller(config)# interface gigabitethernet1/0/2
Controller(config-if)# switchport
*Jan  3 18:04:17.007: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/1, changed state to down.
NOTE: If this message appears, this interface changes to layer 2, so that you can apply the
 filter.
Controller(config-if)# ip igmp filter 40
```

You can verify your setting by using the **show running-config** privileged EXEC command and by specifying an interface.

Related Commands

Command	Description
ip igmp profile	configures and enters IGMP Filter Profile configuration mode
show ip dhcp snooping statistics	displays DHCP snooping statistics

ip igmp max-groups

Use the **ip igmp max-groups** interface configuration command on the controller stack or on a standalone controller to set the maximum number of Internet Group Management Protocol (IGMP) groups that a Layer 2 interface can join or to configure the IGMP throttling action when the maximum number of entries is in the forwarding table. Use the no form of this command to set the maximum back to the default, which is to have no maximum limit, or to return to the default throttling action, which is to drop the report.

ip igmp max-groups [*max number* | **action** { **deny** | **replace**}]

no ip igmp max-groups {*max number* | **action**}

Syntax Description

max number	The maximum number of IGMP groups that an interface can join. The range is 0 to 4294967294. The default is no limit.
action deny	When the maximum number of entries is in the IGMP snooping forwarding table, drop the next IGMP join report. This is the default action.
action replace	When the maximum number of entries is in the IGMP snooping forwarding table, replace the existing group with the new group for which the IGMP report was received.

Command Default

The default maximum number of groups is no limit.

After the controller learns the maximum number of IGMP group entries on an interface, the default throttling action is to drop the next IGMP report that the interface receives and to not add an entry for the IGMP group to the interface.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You can use this command only on Layer 2 physical interfaces and on logical EtherChannel interfaces. You cannot set IGMP maximum groups for routed ports, switch virtual interfaces (SVIs), or ports that belong to an EtherChannel group.

Follow these guidelines when configuring the IGMP throttling action:

- If you configure the throttling action as deny and set the maximum group limitation, the entries that were previously in the forwarding table are not removed but are aged out. After these entries are aged out, when the maximum number of entries is in the forwarding table, the controller drops the next IGMP report received on the interface.

- If you configure the throttling action as replace and set the maximum group limitation, the entries that were previously in the forwarding table are removed. When the maximum number of entries is in the forwarding table, the controller replaces a randomly selected multicast entry with the received IGMP report.
- When the maximum group limitation is set to the default (no maximum), entering the ip igmp max-groups {deny | replace} command has no effect.

Examples

This example shows how to limit to 25 the number of IGMP groups that a port can join:

```
Controller(config)# interface gigabitethernet1/0/2
Controller(config-if)# ip igmp max-groups 25
```

This example shows how to configure the controller to replace the existing group with the new group for which the IGMP report was received when the maximum number of entries is in the forwarding table:

```
Controller(config)# interface gigabitethernet2/0/1
Controller(config-if)# ip igmp max-groups action replace
```

You can verify your setting by using the **show running-config** privileged EXEC command and by specifying an interface.

ip igmp profile

Use the **ip igmp profile** global configuration command on the controller stack or on a standalone controller to create an Internet Group Management Protocol (IGMP) profile and enter IGMP profile configuration mode. From this mode, you can specify the configuration of the IGMP profile to be used for filtering IGMP membership reports from a switchport. Use the **no** form of this command to delete the IGMP profile.

ip igmp profile *profile number*

no ip igmp profile *profile number*

Syntax Description

profile number	The IGMP profile number being configured. The range is from 1 to 4294967295.

Command Default

No IGMP profiles are defined. When configured, the default action for matching an IGMP profile is to deny matching addresses.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was first introduced.

Usage Guidelines

When you are in IGMP profile configuration mode, you can create the profile by using these commands:

- **deny**: specifies that matching addresses are denied; this is the default condition.
- **exit**: exits from igmp-profile configuration mode.
- **no**: negates a command or resets to its defaults.
- **permit**: specifies that matching addresses are permitted.
- **range**: specifies a range of IP addresses for the profile. This can be a single IP address or a range with a start and an end address.

  When entering a range, enter the low IP multicast address, a space, and the high IP multicast address.

You can apply an IGMP profile to one or more Layer 2 interfaces, but each interface can have only one profile applied to it.

Examples

This example shows how to configure IGMP profile 40 that permits the specified range of IP multicast addresses:

```
Controller(config)# ip igmp profile 40
Controller(config-igmp-profile)# permit
Controller(config-igmp-profile)# range 233.1.1.1 233.255.255.255
```

You can verify your settings by using the **show ip igmp profile** privileged EXEC command.

Related Commands

Command	Description
ip igmp filter	applies IGMP profile to the interface
show ip igmp profile	Displays configured IGMP profiles specified by the command

ip igmp snooping

To globally enable Internet Group Management Protocol (IGMP) snooping on the controller or to enable it on a per-VLAN basis, use the **ip igmp snooping** global configuration command on the controller stack or on a standalone controller. To return to the default setting, use the **no** form of this command.

ip igmp snooping [**vlan** *vlan-id*]

no ip igmp snooping [**vlan** *vlan-id*]

Syntax Description

vlan *vlan-id*	(Optional) Enables IGMP snooping on the specified VLAN. The range is 1 to 1001 and 1006 to 4094.

Command Default

IGMP snooping is globally enabled on the controller.

IGMP snooping is enabled on VLAN interfaces.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

When IGMP snooping is enabled globally, it is enabled in all of the existing VLAN interfaces. When IGMP snooping is globally disabled, it is disabled on all of the existing VLAN interfaces.

VLAN IDs 1002 to 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in IGMP snooping.

Examples

This example shows how to globally enable IGMP snooping:

```
Controller(config)# ip igmp snooping
```

This example shows how to enable IGMP snooping on VLAN 1:

```
Controller(config)# ip igmp snooping vlan 1
```

You can verify your settings by entering the **show ip igmp snooping** privileged EXEC command.

Related Commands

Command	Description
ip igmp snooping report-suppression	Enables IGMP report suppression.
show ip igmp snooping	Displays IGMP snooping configurations.

ip igmp snooping last-member-query-count

To configure how often Internet Group Management Protocol (IGMP) snooping will send query messages in response to receiving an IGMP leave message, use the **ip igmp snooping last-member-query-count** command in global configuration or bridge domain configuration mode. To set *count* to the default value, use the **no** form of the command.

ip igmp snooping [**vlan** *vlan-id*] **last-member-query-count** *count*

no ip igmp snooping [**vlan** *vlan-id*] **last-member-query-count** *count*

Syntax Description

vlan *vlan-id*	(Optional) Sets the count value on a specific VLAN ID. The range is from 1 to 1001. Do not enter leading zeroes.
count	The interval at which query messages are sent, in milliseconds. The range is from 1 to 7. The default is 2.

Command Default

A query is sent every 2 milliseconds.

Command Modes

Global configuration

Bridge domain configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

When a multicast host leaves a group, the host sends an IGMP leave message. To check if this host is the last to leave the group, IGMP query messages are sent when the leave message is seen until the **last-member-query-interval** timeout period expires. If no response to the last-member queries are received before the timeout period expires, the group record is deleted.

Use the **ip igmp snooping last-member-query-interval** command to configure the timeout period.

When both IGMP snooping immediate-leave processing and the query count are configured, immediate-leave processing takes precedence.

Note Do not set the count to 1 because the loss of a single packet (the query packet from the controller to the host or the report packet from the host to the controller) may result in traffic forwarding being stopped even if there is still a receiver. Traffic continues to be forwarded after the next general query is sent by the controller, but the interval during which a receiver may not receive the query could be as long as 1 minute (with the default query interval).

The leave latency in Cisco IOS software may increase by up to one last-member-query-interval (LMQI) value when the controller is processing more than one leave within a LMQI. In this case, the average leave latency is determined by the (count + 0.5) * LMQI. The result is that the default leave latency can range from 2.0 to 3.0 seconds with an average of 2.5 seconds under a higher load of IGMP leave processing. The leave latency under load for the minimum LMQI value of 100 milliseconds and a count of 1 is from 100 to 200 milliseconds, with an average of 150 milliseconds. This is done to limit the impact of higher rates of IGMP leave messages.

Examples

The following example sets the last member query count to 5:

```
Controller(config)# ip igmp snooping last-member-query-count 5
```

ip igmp snooping querier

To globally enable the Internet Group Management Protocol (IGMP) querier function in Layer 2 networks, use the **ip igmp snooping querier** global configuration command on the controller stack or on a standalone controller . Use the command with keywords to enable and configure the IGMP querier feature on a VLAN interface. To return to the default settings, use the **no** form of this command.

ip igmp snooping [**vlan** *vlan-id*] **querier** [**address** *ip-address* | **max-response-time** *response-time* | **query-interval** *interval-count* | **tcn query** {**count** *count* | **interval** *interval*} | **timer expiry** *expiry-time* | **version** *version*]

no ip igmp snooping [**vlan** *vlan-id*] **querier** [**address** | **max-response-time** | **query-interval** | **tcn query** {**count** | **interval**} | **timer expiry** *expiry-time* | **version**]

Syntax Description

vlan *vlan-id*	(Optional) Enables IGMP snooping and the IGMP querier function on the specified VLAN. The range is 1 to 1001 and 1006 to 4094.
address *ip-address*	(Optional) Specifies a source IP address. If you do not specify an IP address, the querier tries to use the global IP address configured for the IGMP querier.
max-response-time *response-time*	(Optional) Sets the maximum time to wait for an IGMP querier report. The range is 1 to 25 seconds.
query-interval *interval-count*	(Optional) Sets the interval between IGMP queriers. The range is 1 to 18000 seconds.
tcn query	(Optional) Sets parameters related to Topology Change Notifications (TCNs).
count *count*	Sets the number of TCN queries to be executed during the TCN interval time. The range is 1 to 10.
interval *interval*	Sets the TCN query interval time. The range is 1 to 255.
timer expiry *expiry-time*	(Optional) Sets the length of time until the IGMP querier expires. The range is 60 to 300 seconds.
version *version*	(Optional) Selects the IGMP version number that the querier feature uses. Select 1 or 2.

Command Default

The IGMP snooping querier feature is globally disabled on the controller.

When enabled, the IGMP snooping querier disables itself if it detects IGMP traffic from a multicast-enabled device.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Use this command to enable IGMP snooping to detect the IGMP version and IP address of a device that sends IGMP query messages, which is also called a querier.

By default, the IGMP snooping querier is configured to detect devices that use IGMP Version 2 (IGMPv2) but does not detect clients that are using IGMP Version 1 (IGMPv1). You can manually configure the max-response-time value when devices use IGMPv2. You cannot configure the max-response-time when devices use IGMPv1. (The value cannot be configured and is set to zero).

Non-RFC compliant devices running IGMPv1 might reject IGMP general query messages that have a non-zero value as the max-response-time value. If you want the devices to accept the IGMP general query messages, configure the IGMP snooping querier to run IGMPv1.

VLAN IDs 1002 to 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in IGMP snooping.

Examples

This example shows how to globally enable the IGMP snooping querier feature:

```
Controller(config)# ip igmp snooping querier
```

This example shows how to set the IGMP snooping querier maximum response time to 25 seconds:

```
Controller(config)# ip igmp snooping querier max-response-time 25
```

This example shows how to set the IGMP snooping querier interval time to 60 seconds:

```
Controller(config)# ip igmp snooping querier query-interval 60
```

This example shows how to set the IGMP snooping querier TCN query count to 25:

```
Controller(config)# ip igmp snooping querier tcn count 25
```

This example shows how to set the IGMP snooping querier timeout to 60 seconds:

```
Controller(config)# ip igmp snooping querier timeout expiry 60
```

This example shows how to set the IGMP snooping querier feature to version 2:

```
Controller(config)# ip igmp snooping querier version 2
```

You can verify your settings by entering the **show ip igmp snooping** privileged EXEC command.

Related Commands

Command	Description
ip igmp snooping report-suppression	Enables IGMP report suppression.
show ip igmp snooping	Displays IGMP snooping configurations.
show ip igmp snooping groups	Displays the IGMP snooping multicast table.

ip igmp snooping report-suppression

To enable Internet Group Management Protocol (IGMP) report suppression, use the **ip igmp snooping report-suppression** global configuration command on the controller stack or on a standalone controller. To disable IGMP report suppression and to forward all IGMP reports to multicast routers, use the **no** form of this command.

ip igmp snooping report-suppression

no ip igmp snooping report-suppression

Syntax Description

This command has no arguments or keywords.

Command Default

IGMP report suppression is enabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

IGMP report suppression is supported only when the multicast query has IGMPv1 and IGMPv2 reports. This feature is not supported when the query includes IGMPv3 reports.

The controller uses IGMP report suppression to forward only one IGMP report per multicast router query to multicast devices. When IGMP router suppression is enabled (the default), the controller sends the first IGMP report from all hosts for a group to all the multicast routers. The controller does not send the remaining IGMP reports for the group to the multicast routers. This feature prevents duplicate reports from being sent to the multicast devices.

If the multicast router query includes requests only for IGMPv1 and IGMPv2 reports, the controller forwards only the first IGMPv1 or IGMPv2 report from all hosts for a group to all of the multicast routers. If the multicast router query also includes requests for IGMPv3 reports, the controller forwards all IGMPv1, IGMPv2, and IGMPv3 reports for a group to the multicast devices.

If you disable IGMP report suppression by entering the **no ip igmp snooping report-suppression** command, all IGMP reports are forwarded to all of the multicast routers.

Examples

This example shows how to disable report suppression:

```
Controller(config)# no ip igmp snooping report-suppression
```

You can verify your settings by entering the **show ip igmp snooping** privileged EXEC command.

Related Commands

Command	Description
show ip igmp snooping	Displays IGMP snooping configurations.

ip igmp snooping vlan mrouter

To add a multicast router port, use the **ip igmp snooping mrouter** global configuration command on the controller stack or on a standalone controller. To return to the default settings, use the **no** form of this command.

Command Default

By default, there are no multicast router ports.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

VLAN IDs 1002 to 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in IGMP snooping.

The configuration is saved in NVRAM.

Examples

This example shows how to configure a port as a multicast router port:

```
Controller(config)# ip igmp snooping vlan 1 mrouter interface gigabitethernet1/0/2
```

You can verify your settings by entering the **show ip igmp snooping** privileged EXEC command.

Related Commands

Command	Description
ip igmp snooping report-suppression	Enables IGMP report suppression.
show ip igmp snooping	Displays IGMP snooping configurations.
show ip igmp snooping groups	Displays the IGMP snooping multicast table.
show ip igmp snooping mrouter	Displays the IGMP snooping multicast router ports.
show ip igmp snooping querier	Displays the configuration and operation information for the IGMP querier.

ip igmp snooping vlan static

To enable Internet Group Management Protocol (IGMP) snooping and to statically add a Layer 2 port as a member of a multicast group, use the **ip igmp snooping static** global configuration command on the controller stack or on a standalone controller. Use the **no** form of this command to remove ports specified as members of a static multicast group.

ip igmp snooping vlan *vlan-id* **static** *ip-address* **interface** *interface-id*

no ip igmp snooping vlan *vlan-id* **static** *ip-address* **interface** *interface-id*

Syntax Description

vlan-id	Enables IGMP snooping on the specified VLAN. The range is 1 to 1001 and 1006 to 4094.
ip-address	Adds a Layer 2 port as a member of a multicast group with the specified group IP address.
interface *interface-id*	Specifies the interface of the member port. The arguments have these meanings: • *fastethernet interface number*—A Fast Ethernet IEEE 802.3 interface. • *gigabitethernet interface number*—A Gigabit Ethernet IEEE 802.3z interface. • *tengigabitethernet interface number*—A 10-Gigabit Ethernet IEEE 802.3z interface. • *port-channel interface number*—A channel interface. The range is 0 to 48.

Command Default

By default, there are no ports statically configured as members of a multicast group.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

VLAN IDs 1002 to 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in IGMP snooping.

The configuration is saved in NVRAM.

Examples

This example shows how to statically configure a host on an interface:

```
Controller(config)# ip igmp snooping vlan 1 static 200.000.000.000 interface
gigabitEthernet1/0/1
Configuring port gigabitethernet1/0/1 on group 200.000.000.000
```

You can verify your settings by entering the **show ip igmp snooping** privileged EXEC command.

Related Commands

Command	Description
ip igmp snooping report-suppression	Enables IGMP report suppression.
show ip igmp snooping	Displays IGMP snooping configurations.
show ip igmp snooping groups	Displays the IGMP snooping multicast table.
show ip igmp snooping mrouter	Displays the IGMP snooping multicast router ports.
show ip igmp snooping querier	Displays the configuration and operation information for the IGMP querier.

ip multicast vlan

To configure IP multicast on a single VLAN, use the **ip multicast vlan** command in global configuration mode. To remove the VLAN from WLAN, use the no form of the command.

ip multicast vlan {*vlan-name* | *vlan-id*}

no ip multicast vlan{*vlan-name* | *vlan-id*}

Syntax Description

vlan-name	Specifies the VLAN name.
vlan-id	Specifies the VLAN ID.

Command Default

Disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

TBD

Examples

```
Controller# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)# ip multicast vlan vlan_id01
```

show ip igmp filter

To display Internet Group Management Protocol (IGMP) filter information, use the **show ip igmp filter** command in privileged EXEC command mode.

show ip igmp [**vrf** *vrf-name*] **filter**

Syntax Description

vrf	(Optional) Supports the multicast VPN routing and forwarding (VRF) instance.
vrf-name	vrf-name

Command Default

IGMP filters are enabled by default.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The **show ip igmp filter** command displays information about all filters defined on the controller.

Examples

The following is sample output from the **show ip igmp filter** command:

```
Controller# show ip igmp filter

IGMP filter enabled
```

show ip igmp profile

To display all configured Internet Group Management Protocol (IGMP) profiles or a specified IGMP profile, use the **show ip igmp profile** privileged EXEC command.

show ip igmp [**vrf** *vrf-name*] **profile** [*profile number*]

Syntax Description

vrf *vrf-name*	(Optional) Supports the multicast VPN routing and forwarding (VRF) instance.
profile number	(Optional) The IGMP profile number to be displayed. The range is 1 to 4294967295. If no profile number is entered, all IGMP profiles are displayed.

Command Default

IGMP profiles undefined by default.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

None

Examples

The following example shows the output of the **show ip igmp profile** privileged EXEC command for Profile Number 40 on the controller:

```
Controller# show ip igmp profile 40
IGMP Profile 40
    permit
    range 233.1.1.1 233.255.255.255
```

This example shows the output of the **show ip igmp profile** privileged EXEC command for all profiles configured on the controller:

```
Controller# show ip igmp profile

IGMP Profile 3
    range 230.9.9.0 230.9.9.0
IGMP Profile 4
    permit
    range 229.9.9.0 229.255.255.255
```

Related Commands

Command	Description
ip igmp profile	configures and enters IGMP Filter Profile configuration mode

show ip igmp snooping

To display the Internet Group Management Protocol (IGMP) snooping configuration of the controller or the VLAN, use the **show ip igmp snooping** command in user or privileged EXEC command mode.

show ip igmp snooping [**groups** | **mrouter** | **querier**] [**vlan** *vlan-id*] [**detail**]

Syntax Description

vlan *vlan-id*	(Optional) Specifies a VLAN; the range is 1 to 1001 and 1006 to 4094.
detail	(Optional) Displays operational state information.

Command Default

None

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Use this command to display snooping configuration for the controller or for a specific VLAN.

VLAN IDs 1002 to 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in IGMP snooping.

Expressions are case sensitive. For example, if you enter | exclude output, the lines that contain output do not appear, but the lines that contain Output appear.

Examples

This is an example of output from the **show ip igmp snooping vlan 1** command. It shows snooping characteristics for a specific VLAN:

```
Controller# show ip igmp snooping vlan 1

Global IGMP Snooping configuration:
-------------------------------------------
IGMP snooping                : Enabled
IGMPv3 snooping (minimal)    : Enabled
Report suppression           : Enabled
TCN solicit query            : Disabled
TCN flood query count        : 2
Robustness variable          : 2
Last member query count      : 2
Last member query interval   : 1000

Vlan 1:
--------
IGMP snooping                        : Enabled
IGMPv2 immediate leave               : Disabled
```

```
Multicast router learning mode      : pim-dvmrp
CGMP interoperability mode          : IGMP_ONLY
Robustness variable                 : 2
Last member query count             : 2
Last member query interval          : 1000
```

This is an example of output from the **show ip igmp snooping** command. It displays snooping characteristics for all VLANs on the controller:

```
Controller# show ip igmp snooping
Global IGMP Snooping configuration:
-------------------------------------------
IGMP snooping                : Enabled
IGMPv3 snooping (minimal)    : Enabled
Report suppression           : Enabled
TCN solicit query            : Disabled
TCN flood query count        : 2
Robustness variable          : 2
Last member query count      : 2
Last member query interval   : 1000

Vlan 1:
--------
IGMP snooping                          : Enabled
IGMPv2 immediate leave                 : Disabled
Multicast router learning mode         : pim-dvmrp
CGMP interoperability mode             : IGMP_ONLY
Robustness variable                    : 2
Last member query count                : 2
Last member query interval             : 1000
Vlan 2:
--------
IGMP snooping                          : Enabled
IGMPv2 immediate leave                 : Disabled
Multicast router learning mode         : pim-dvmrp
CGMP interoperability mode             : IGMP_ONLY
Robustness variable                    : 2
Last member query count                : 2
Last member query interval             : 1000
<output truncated>
```

Related Commands

Command	Description
ip igmp snooping	Enables IGMP snooping.
show ip igmp snooping groups	Displays the IGMP snooping multicast table.
show ip igmp snooping mrouter	Displays the IGMP snooping multicast router ports.
show ip igmp snooping querier	Displays the configuration and operation information for the IGMP querier.

show ip igmp snooping groups

To display the Internet Group Management Protocol (IGMP) snooping multicast table for the controller or the multicast information, use the **show ip igmp snooping groups** privileged EXEC command . Use with the **vlan** keyword to display the multicast table for a specified multicast VLAN or specific multicast information.

show ip igmp snooping groups [**vlan** *vlan-id*] [[**dynamic** | **user**] [**count**] | *ip_address*]

Syntax Description

vlan *vlan-id*	(Optional) Specifies a VLAN; the range is 1 to 1001 and 1006 to 4094.
dynamic	(Optional) Displays IGMP Snooping learned group information.
user	(Optional) Displays user configured group information.
count	(Optional) Displays the total number of entries for the specified command options instead of the actual entries.
ip_address	(Optional) Characteristics of the multicast group with the specified group IP address.

Command Default

None

Command Modes

Privileged EXEC

User EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Use this command to display multicast information or the multicast table.

Expressions are case sensitive. For example, if you enter | exclude output, the lines that contain output do not appear, but the lines that contain Output appear.

Examples

This is an example of output from the **show ip igmp snooping groups** command without any keywords. It displays the multicast table for the controller:

```
Controller# show ip igmp snooping groups
Vlan      Group           Type        Version     Port List
------------------------------------------------------------
1         224.1.4.4       igmp                    Gi1/0/11
1         224.1.4.5       igmp                    Gi1/0/11
2         224.0.1.40      igmp        v2          Gi1/0/15
```

```
104       224.1.4.2      igmp        v2          Gi2/0/1, Gi2/0/2
104       224.1.4.3      igmp        v2          Gi2/0/1, Gi2/0/2
```

This is an example of output from the **show ip igmp snooping groups count** command. It displays the total number of multicast groups on the controller:

```
Controller# show ip igmp snooping groups count
Total number of multicast groups: 2
```

This is an example of output from the **show ip igmp snooping groups vlan vlan-id ip-address** command. It shows the entries for the group with the specified IP address:

```
Controller# show ip igmp snooping groups vlan 104 224.1.4.2
Vlan      Group           Type        Version     Port List
-----------------------------------------------------------
104       224.1.4.2      igmp        v2          Gi2/0/1, Gi1/0/15
```

Related Commands

Command	Description
ip igmp snooping	Enables IGMP snooping.
show ip igmp snooping	Displays IGMP snooping configurations.

show ip igmp snooping igmpv2-tracking

To display group and IP address entries, use the **show ip igmp snooping igmpv2-tracking** command in privileged EXEC mode.

Note The command displays group and IP address entries only for wireless multicast IGMP joins and not for wired joins. This command also displays output only if wireless multicast is enabled.

show ip igmp snooping igmpv2-tracking

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The command displays group and IP address entries only for wireless multicast IGMP joins and not for wired joins. This command also displays output only if wireless multicast is enabled.

show ip igmp snooping mrouter

To display the Internet Group Management Protocol (IGMP) snooping dynamically learned and manually configured multicast router ports for the controller or for the specified multicast VLAN, use the **show ip igmp snooping mrouter** privileged EXEC command.

show ip igmp snooping mrouter [**vlan** *vlan-id*]

Syntax Description

vlan *vlan-id*	(Optional) Specifies a VLAN; the range is 1 to 1001 and 1006 to 4094.

Command Default

None

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Use this command to display multicast router ports on the controller or for a specific VLAN.

VLAN IDs 1002 to 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in IGMP snooping.

When multicast VLAN registration (MVR) is enabled, the **show ip igmp snooping mrouter** command displays MVR multicast router information and IGMP snooping information.

Expressions are case sensitive. For example, if you enter | exclude output, the lines that contain output do not appear, but the lines that contain Output appear.

Examples

This is an example of output from the **show ip igmp snooping mrouter** command. It shows how to display multicast router ports on the controller:

```
Controller# show ip igmp snooping mrouter
Vlan    ports
----    -----
   1    Gi2/0/1(dynamic)
```

Related Commands

Command	Description
ip igmp snooping	Enables IGMP snooping.
show ip igmp snooping	Displays IGMP snooping configurations.

Command	Description
show ip igmp snooping groups	Displays the IGMP snooping multicast table.

show ip igmp snooping querier

To display the configuration and operation information for the IGMP querier configured on a controller, use the **show ip igmp snooping querier** user EXEC command.

show ip igmp snooping querier [**vlan** *vlan-id*] [**detail**]

Syntax Description

vlan *vlan-id*	(Optional) Specifies a VLAN; the range is 1 to 1001 and 1006 to 4094. Use the detail keyword to display detailed information.
detail	(Optional) Displays detailed IGMP querier information.

Command Default

None

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Use the **show ip igmp snooping querier** command to display the IGMP version and the IP address of a detected device, also called a querier, that sends IGMP query messages. A subnet can have multiple multicast routers but has only one IGMP querier. In a subnet running IGMPv2, one of the multicast routers is elected as the querier. The querier can be a Layer 3 controller.

The **show ip igmp snooping querier** command output also shows the VLAN and the interface on which the querier was detected. If the querier is the controller, the output shows the Port field as Router. If the querier is a router, the output shows the port number on which the querier is learned in the Port field.

The **show ip igmp snooping querier detail** user EXEC command is similar to the **show ip igmp snooping querier** command. However, the **show ip igmp snooping querier** command displays only the device IP address most recently detected by the controller querier.

The **show ip igmp snooping querier detail** command displays the device IP address most recently detected by the controller querier and this additional information:

- The elected IGMP querier in the VLAN
- The configuration and operational information pertaining to the controller querier (if any) that is configured in the VLAN

Expressions are case sensitive. For example, if you enter | exclude output, the lines that contain output do not appear, but the lines that contain Output appear.

Examples

This is an example of output from the **show ip igmp snooping querier** command:

```
Controller> show ip igmp snooping querier
Vlan      IP Address      IGMP Version        Port
---------------------------------------------------
1         172.20.50.11    v3                  Gi1/0/1
2         172.20.40.20    v2                  Router
```

This is an example of output from the **show ip igmp snooping querier detail** command:

```
Controller> show ip igmp snooping querier detail
Vlan      IP Address      IGMP Version    Port
-------------------------------------------------------------
1         1.1.1.1         v2              Fa8/0/1
Global IGMP controller querier status
-------------------------------------------------------
admin state                    : Enabled
admin version                  : 2
source IP address              : 0.0.0.0
query-interval (sec)           : 60
max-response-time (sec)        : 10
querier-timeout (sec)          : 120
tcn query count                : 2
tcn query interval (sec)       : 10
Vlan 1:   IGMP controller querier status
-------------------------------------------------------
elected querier is 1.1.1.1          on port Fa8/0/1
-------------------------------------------------------
admin state                    : Enabled
admin version                  : 2
source IP address              : 10.1.1.65
query-interval (sec)           : 60
max-response-time (sec)        : 10
querier-timeout (sec)          : 120
tcn query count                : 2
tcn query interval (sec)       : 10
operational state              : Non-Querier
operational version            : 2
tcn query pending count        : 0
```

Related Commands

Command	Description
ip igmp snooping	Enables IGMP snooping.
ip igmp snooping querier	Globally enables the IGMP querier function.
show ip igmp snooping	Displays IGMP snooping configurations.

show ip igmp snooping wireless mcast-spi-count

To display the statistics of number of multicast SPIs per MGID sent to the controller, use the **show ip igmp snooping wireless mcast-spi-count** command in privileged EXEC mode.

show ip igmp snooping wireless mcast-spi-count

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

None

Examples

This is an example of output from the **show ip igmp snooping wireless mcast-spi-count** command.

```
Controller# show ip igmp snooping wireless mcast-spi-count

Stats for Mcast Client Add/Delete SPI Messages Sent to WCM

MGID    ADD MSGs        Del MSGs
---------------------------------
```

show ip igmp snooping wireless mgid

To display multicast group ID (MGID) mappings, use the **show ip igmp snooping wireless mgid** command in privileged EXEC mode.

show ip igmp snooping wireless mgid

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

None

Examples

This is an example of output from the **show ip igmp snooping wireless mgid** command.

```
Controller# show ip igmp snooping wireless mgid

Total number of L2-MGIDs    = 0

Total number of MCAST MGIDs = 0

 Wireless multicast is Enabled in the system
 Vlan     bcast   nonip-mcast   mcast    mgid    Stdby Flags
 1     Disabled   Disabled   Enabled    Disabled  0:0:1:0
 25    Disabled   Disabled   Enabled    Disabled  0:0:1:0
 34    Disabled   Disabled   Enabled    Disabled  0:0:1:0
 200   Disabled   Disabled   Enabled    Disabled  0:0:1:0
 1002  Enabled    Enabled    Enabled    Disabled  0:0:1:0
 1003  Enabled    Enabled    Enabled    Disabled  0:0:1:0
 1004  Enabled    Enabled    Enabled    Disabled  0:0:1:0
 1005  Enabled    Enabled    Enabled    Disabled  0:0:1:0

Index  MGID                 (S, G, V)
-----------------------------------------------------------
```

show wireless multicast

To display wireless multicast information, use the **show wireless multicast** command in privileged EXEC mode.

show wireless multicast [**source** *source-ip* **group** *group-ip* **vlan** *vlan-id* | **group** *group-ip* **vlan** *vlan-id*]

Syntax Description

source *source-ip*	(Optional) Specifies the source IPv4/IPv6 Address of multicast traffic.
group *group-ip* **vlan** *vlan-id*	(Optional) Specifies the destination group and group IP of mutlicast traffic and displays the client information on VLAN with the specific VLAN ID.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

None

Examples

This example shows how to display the wireless multicast information.

```
Controller# show wireless multicast

Multicast                                 : Enabled
AP Capwap Multicast                       : Unicast
Wireless Broadcast                        : Disabled
Wireless Multicast non-ip-mcast           : Disabled

Vlan        Non-ip-mcast     Broadcast        MGID
------------------------------------------------------------
1           Enabled          Enabled          Enabled
2           Enabled          Enabled          Disabled
94          Enabled          Enabled          Disabled
```

show wireless multicast group

To display the information of the wireless-multicast non-ip VLANs or the group, use the **show wireless multicast group** command in privileged EXEC mode.

show wireless multicast group {**summary** | *group-ip* **vlan** *vlan-id*}

Syntax Description

summary	Displays wireless-multicast non-ip group summary.
group-ip	Specifies the group IP address.
vlan *vlan-id*	Specifies the destination group IPv4/IPv6 Address of multicast traffic.

Command Default

None.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

None.

Examples

This example shows how to display the wireless-multicast non-ip group summary.

```
Controller# show wireless multicast group summary
```

wireless multicast

To enable Ethernet Multicast Support, use the **wireless multicast** command.

wireless multicast [**non-ip** [**vlan** *vlan-id*]]

Syntax Description

non-ip	Configures multicast non-ip support.
vlan *vlan-id*	Specifies multicast non-ip for a VLAN. The interface number ranges between 1 and 4095.

Command Default

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

TBD

Examples

This example shows how to configure multicast non-ip VLAN.

```
Controller# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)# wireless multicast non-ip vlan 20
```

PART VII

Security

Security Commands

aaa accounting dot1x

To enable authentication, authorization, and accounting (AAA) accounting and to create method lists defining specific accounting methods on a per-line or per-interface basis for IEEE 802.1x sessions, use the **aaa accounting dot1x** global configuration command. Use the **no** form of this command to disable IEEE 802.1x accounting.

aaa accounting dot1x {*name* | **default** } **start-stop** {**broadcast group** {*name* | **radius** | **tacacs+**} [**group** {*name* | **radius** | **tacacs+**} ...] | **group** {*name* | **radius** | **tacacs+**} [**group** {*name* | **radius** | **tacacs+**}...]}

no aaa accounting dot1x {*name* | **default** }

Syntax Description

name	Name of a server group. This is optional when you enter it after the **broadcast group** and **group** keywords.
default	Specifies the accounting methods that follow as the default list for accounting services.
start-stop	Sends a start accounting notice at the beginning of a process and a stop accounting notice at the end of a process. The start accounting record is sent in the background. The requested user process begins regardless of whether or not the start accounting notice was received by the accounting server.
broadcast	Enables accounting records to be sent to multiple AAA servers and sends accounting records to the first server in each group. If the first server is unavailable, the switch uses the list of backup servers to identify the first server.
group	Specifies the server group to be used for accounting services. These are valid server group names: • *name* **—** Name of a server group. • **radius —** Lists of all RADIUS hosts. • **tacacs+ —** Lists of all TACACS+ hosts. The **group** keyword is optional when you enter it after the **broadcast group** and **group** keywords. You can enter more than optional **group** keyword.
radius	(Optional) Enables RADIUS accounting.
tacacs+	(Optional) Enables TACACS+ accounting.

Command Default

AAA accounting is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

This command requires access to a RADIUS server.

We recommend that you enter the **dot1x reauthentication** interface configuration command before configuring IEEE 802.1x RADIUS accounting on an interface.

Examples

This example shows how to configure IEEE 802.1x accounting:

```
Controller(config)# aaa new-model
Controller(config)# aaa accounting dot1x default start-stop group radius
```

aaa accounting identity

To enable authentication, authorization, and accounting (AAA) accounting for IEEE 802.1x, MAC authentication bypass (MAB), and web authentication sessions, use the **aaa accounting identity** global configuration command. Use the **no** form of this command to disable IEEE 802.1x accounting.

aaa accounting identity {*name* | **default** } **start-stop** {**broadcast group** {*name* | **radius** | **tacacs+**} [**group** {*name* | **radius** | **tacacs+**} ...] | **group** {*name* | **radius** | **tacacs+**} [**group** {*name* | **radius** | **tacacs+**}...]}

no aaa accounting identity {*name* | **default** }

Syntax Description

name	Name of a server group. This is optional when you enter it after the **broadcast group** and **group** keywords.
default	Uses the accounting methods that follow as the default list for accounting services.
start-stop	Sends a start accounting notice at the beginning of a process and a stop accounting notice at the end of a process. The start accounting record is sent in the background. The requested-user process begins regardless of whether or not the start accounting notice was received by the accounting server.
broadcast	Enables accounting records to be sent to multiple AAA servers and send accounting records to the first server in each group. If the first server is unavailable, the switch uses the list of backup servers to identify the first server.
group	Specifies the server group to be used for accounting services. These are valid server group names: • *name* **—** Name of a server group. • **radius —** Lists of all RADIUS hosts. • **tacacs+ —** Lists of all TACACS+ hosts. The **group** keyword is optional when you enter it after the **broadcast group** and **group** keywords. You can enter more than optional **group** keyword.
radius	(Optional) Enables RADIUS authorization.
tacacs+	(Optional) Enables TACACS+ accounting.

Command Default

AAA accounting is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

To enable AAA accounting identity, you need to enable policy mode. To enable policy mode, enter the **authentication display new-style** command in privileged EXEC mode.

Examples

This example shows how to configure IEEE 802.1x accounting identity:

```
Controller# authentication display new-style

Please note that while you can revert to legacy style
configuration at any time unless you have explicitly
entered new-style configuration, the following caveats
should be carefully read and understood.

(1) If you save the config in this mode, it will be written
    to NVRAM in NEW-style config, and if you subsequently
    reload the router without reverting to legacy config and
    saving that, you will no longer be able to revert.

(2) In this and legacy mode, Webauth is not IPv6-capable. It
    will only become IPv6-capable once you have entered new-
    style config manually, or have reloaded with config saved
    in 'authentication display new' mode.

Controller# configure terminal
Controller(config)# aaa accounting identity default start-stop group radius
```

aaa authentication dot1x

To specify the authentication, authorization, and accounting (AAA) method to use on ports complying with the IEEE 802.1x authentication, use the **aaa authentication dot1x** global configuration command on the switch stack or on a standalone switch. Use the **no** form of this command to disable authentication.

aaa authentication dot1x {**default**} *method1*

no aaa authentication dot1x {**default**} *method1*

Syntax Description

default	The default method when a user logs in. Use the listed authentication method that follows this argument.
method1	Specifies the server authentication. Enter the **group radius** keywords to use the list of all RADIUS servers for authentication. **Note** Though other keywords are visible in the command-line help strings, only the **default** and **group radius** keywords are supported.

Command Default

No authentication is performed.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The **method** argument identifies the method that the authentication algorithm tries in the specified sequence to validate the password provided by the client. The only method that is IEEE 802.1x-compliant is the **group radius** method, in which the client data is validated against a RADIUS authentication server.

If you specify **group radius**, you must configure the RADIUS server by entering the **radius-server host** global configuration command.

Use the **show running-config** privileged EXEC command to display the configured lists of authentication methods.

Examples

This example shows how to enable AAA and how to create an IEEE 802.1x-compliant authentication list. This authentication first tries to contact a RADIUS server. If this action returns an error, the user is not allowed access to the network.

```
Controller(config)# aaa new-model
Controller(config)# aaa authentication dot1x default group radius
```

aaa authorization

To set the parameters that restrict user access to a network, use the **aaa authorization** command in global configuration mode. To remove the parameters, use the **no** form of this command.

aaa authorization { **auth-proxy** | **cache** | **commands** *level* | **config-commands** | **configuration** | **console** | **credential-download** | **exec** | **multicast** | **network** | **onep** | **policy-if** | **prepaid** | **radius-proxy** | **reverse-access** | **subscriber-service** | **template**} {**default** | *list_name* } [*method1* [*method2* ...]]

aaa authorization { **auth-proxy** | **cache** | **commands** *level* | **config-commands** | **configuration** | **console** | **credential-download** | **exec** | **multicast** | **network** | **reverse-access** |**template**} {**default** | *list_name* } [*method1* [*method2* ...]]

no aaa authorization { **auth-proxy** | **cache** | **commands** *level* | **config-commands** | **configuration** | **console** | **credential-download** | **exec** | **multicast** | **network** | **reverse-access** |**template**} {**default** | *list_name* } [*method1* [*method2* ...]]

Syntax Description

auth-proxy	Runs authorization for authentication proxy services.
cache	Configures the authentication, authorization, and accounting (AAA) server.
commands	Runs authorization for all commands at the specified privilege level.
level	Specific command level that should be authorized. Valid entries are 0 through 15.
config-commands	Runs authorization to determine whether commands entered in configuration mode are authorized.
configuration	Downloads the configuration from the AAA server.
console	Enables the console authorization for the AAA server.
credential-download	Downloads EAP credential from Local/RADIUS/LDAP.
exec	Enables the console authorization for the AAA server.
multicast	Downloads the multicast configuration from the AAA server.
network	Runs authorization for all network-related service requests, including Serial Line Internet Protocol (SLIP), PPP, PPP Network Control Programs (NCPs), and AppleTalk Remote Access (ARA).
onep	Runs authorization for the ONEP service.
policy-if	Runs authorization for the diameter policy interface application.
prepaid	Runs authorization for diameter prepaid services.
radius-proxy	Runs authorization for proxy services.

reverse-access	Runs authorization for reverse access connections, such as reverse Telnet.
subscriber-service	Runs authorization for iEdge subscriber services such as virtual private dialup network (VPDN).
template	Enables template authorization for the AAA server.
default	Uses the listed authorization methods that follow this keyword as the default list of methods for authorization.
list_name	Character string used to name the list of authorization methods.
method1 [*method2...*]	(Optional) An authorization method or multiple authorization methods to be used for authorization. A method may be any one of the keywords listed in the table below.

Command Default

Authorization is disabled for all actions (equivalent to the method keyword **none**).

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Use the **aaa authorization** command to enable authorization and to create named methods lists, which define authorization methods that can be used when a user accesses the specified function. Method lists for authorization define the ways in which authorization will be performed and the sequence in which these methods will be performed. A method list is a named list that describes the authorization methods (such as RADIUS or TACACS+) that must be used in sequence. Method lists enable you to designate one or more security protocols to be used for authorization, which ensures a backup system in case the initial method fails. Cisco IOS software uses the first method listed to authorize users for specific network services; if that method fails to respond, the Cisco IOS software selects the next method listed in the method list. This process continues until there is successful communication with a listed authorization method, or until all the defined methods are exhausted.

Note The Cisco IOS software attempts authorization with the next listed method only when there is no response from the previous method. If authorization fails at any point in this cycle--meaning that the security server or the local username database responds by denying the user services--the authorization process stops and no other authorization methods are attempted.

If the **aaa authorization** command for a particular authorization type is issued without a specified named method list, the default method list is automatically applied to all interfaces or lines (where this authorization type applies) except those that have a named method list explicitly defined. (A defined method list overrides

the default method list.) If no default method list is defined, then no authorization takes place. The default authorization method list must be used to perform outbound authorization, such as authorizing the download of IP pools from the RADIUS server.

Use the **aaa authorization** command to create a list by entering the values for the *list-name* and the *method* arguments, where *list-name* is any character string used to name this list (excluding all method names) and *method* identifies the list of authorization methods tried in the given sequence.

Note In the table that follows, the **group***group-name*, **group ldap**, **group radius**, and **group tacacs+** methods refer to a set of previously defined RADIUS or TACACS+ servers. Use the **radius-server host** and **tacacs-server host** commands to configure the host servers. Use the **aaa group server radius**, **aaa group server ldap**, and **aaa group server tacacs+** commands to create a named group of servers.

This table describes the method keywords.

Table 10: aaa authorization Methods

Keyword	Description
cache *group-name*	Uses a cache server group for authorization.
group *group-name*	Uses a subset of RADIUS or TACACS+ servers for accounting as defined by the **server group** *group-name* command.
group ldap	Uses the list of all Lightweight Directory Access Protocol (LDAP) servers for authentication.
group radius	Uses the list of all RADIUS servers for authentication as defined by the **aaa group server radius** command.
grouptacacs+	Uses the list of all TACACS+ servers for authentication as defined by the **aaa group server tacacs+** command.
if-authenticated	Allows the user to access the requested function if the user is authenticated. **Note** The **if-authenticated** method is a terminating method. Therefore, if it is listed as a method, any methods listed after it will never be evaluated.
local	Uses the local database for authorization.
none	Indicates that no authorization is performed.

Cisco IOS software supports the following methods for authorization:

- Cache Server Groups — The router consults its cache server groups to authorize specific rights for users.

- If-Authenticated — The user is allowed to access the requested function provided the user has been authenticated successfully.
- Local— The router or access server consults its local database, as defined by the **username** command, to authorize specific rights for users. Only a limited set of functions can be controlled through the local database.
- None — The network access server does not request authorization information; authorization is not performed over this line or interface.
- RADIUS —The network access server requests authorization information from the RADIUS security server group. RADIUS authorization defines specific rights for users by associating attributes, which are stored in a database on the RADIUS server, with the appropriate user.
- TACACS+ — The network access server exchanges authorization information with the TACACS+ security daemon. TACACS+ authorization defines specific rights for users by associating attribute-value (AV) pairs, which are stored in a database on the TACACS+ security server, with the appropriate user.

Method lists are specific to the type of authorization being requested. AAA supports five different types of authorization:

- Commands — Applies to the EXEC mode commands a user issues. Command authorization attempts authorization for all EXEC mode commands, including global configuration commands, associated with a specific privilege level.
- EXEC — Applies to the attributes associated with a user EXEC terminal session.
- Network — Applies to network connections. The network connections can include a PPP, SLIP, or ARA connection.

Note You must configure the **aaa authorization config-commands** command to authorize global configuration commands, including EXEC commands prepended by the **do** command.

- Reverse Access — Applies to reverse Telnet sessions.
- Configuration — Applies to the configuration downloaded from the AAA server.

When you create a named method list, you are defining a particular list of authorization methods for the indicated authorization type.

Once defined, the method lists must be applied to specific lines or interfaces before any of the defined methods are performed.

The authorization command causes a request packet containing a series of AV pairs to be sent to the RADIUS or TACACS daemon as part of the authorization process. The daemon can do one of the following:

- Accept the request as is.
- Make changes to the request.
- Refuse the request and authorization.

For a list of supported RADIUS attributes, see the module RADIUS Attributes. For a list of supported TACACS+ AV pairs, see the module TACACS+ Attribute-Value Pairs.

Note Five commands are associated with privilege level 0: **disable**, **enable**, **exit**, **help**, and **logout**. If you configure AAA authorization for a privilege level greater than 0, these five commands will not be included in the privilege level command set.

Examples

The following example shows how to define the network authorization method list named mygroup, which specifies that RADIUS authorization will be used on serial lines using PPP. If the RADIUS server fails to respond, local network authorization will be performed.

```
Controller(config)#  aaa authorization network mygroup group radius local
```

access-session mac-move deny

To disable MAC move on a controller, use the **access-session mac-move deny** global configuration command. To return to the default setting, use the **no** form of this command.

access-session mac-move deny

no access-session mac-move deny

Syntax Description

This command has no arguments or keywords.

Command Default

MAC move is enabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The **no** form of this command enables authenticated hosts to move between any authentication-enabled ports (MAC authentication bypass [MAB], 802.1x, or Web-auth) on a controller. For example, if there is a device between an authenticated host and port, and that host moves to another port, the authentication session is deleted from the first port, and the host is reauthenticated on the new port.

If MAC move is disabled, and an authenticated host moves to another port, it is not reauthenticated, and a violation error occurs.

Examples

This example shows how to enable MAC move on a controller:

```
Controller(config)# no access-session mac-move deny
```

Related Commands

Command	Description
authentication event	Sets the action for specific authentication events.
authentication fallback	Configures a port to use web authentication as a fallback method for clients that do not support IEEE 802.1x authentication.
authentication host-mode	Sets the authorization manager mode on a port.
authentication open	Enables or disables open access on a port.

Command	Description
authentication order	Sets the order of authentication methods used on a port.
authentication periodic	Enables or disables reauthentication on a port.
authentication port-control	Enables manual control of the port authorization state.
authentication priority	Adds an authentication method to the port-priority list.
authentication timer	Configures the timeout and reauthentication parameters for an 802.1x-enabled port.
authentication violation	Configures the violation modes that occur when a new device connects to a port or when a new device connects to a port with the maximum number of devices already connected to that port.
show authentication	Displays information about authentication manager events on the switch.

action

To set the action for the VLAN access map entry, use the **action** command in access-map configuration mode. To return to the default setting, use the **no** form of this command.

action{**drop**| **forward**}

no action

Syntax Description

drop	Drops the packet when the specified conditions are matched.
forward	Forwards the packet when the specified conditions are matched.

Command Default

The default action is to forward packets.

Command Modes

Access-map configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You enter access-map configuration mode by using the **vlan access-map** global configuration command.

If the action is **drop**, you should define the access map, including configuring any access control list (ACL) names in match clauses, before applying the map to a VLAN, or all packets could be dropped.

In access-map configuration mode, use the **match access-map** configuration command to define the match conditions for a VLAN map. Use the **action** command to set the action that occurs when a packet matches the conditions.

The drop and forward parameters are not used in the **no** form of the command.

You can verify your settings by entering the **show vlan access-map** privileged EXEC command.

Examples

This example shows how to identify and apply a VLAN access map (vmap4) to VLANs 5 and 6 that causes the VLAN to forward an IP packet if the packet matches the conditions defined in access list al2:

```
Controller(config)# vlan access-map vmap4
Controller(config-access-map)# match ip address al2
Controller(config-access-map)# action forward
Controller(config-access-map)# exit
Controller(config)# vlan filter vmap4 vlan-list 5-6
```

Related Commands

Command	Description
show vlan access-map	Displays the VLAN access maps created on the switch.
vlan access-map	Defines a VLAN map and enters access-map configuration mode where you can specify a MAC ACL to match and the action to be taken.

authentication host-mode

To set the authorization manager mode on a port, use the **authentication host-mode** interface configuration command. To return to the default setting, use the **no** form of this command.

authentication host-mode {**multi-auth** | **multi-domain** | **multi-host** | **single-host**}

no authentication host-mode

Syntax Description

multi-auth	Enables multiple-authorization mode (multi-auth mode) on the port.
multi-domain	Enables multiple-domain mode on the port.
multi-host	Enables multiple-host mode on the port.
single-host	Enables single-host mode on the port.

Command Default

Single host mode is enabled.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Single-host mode should be configured if only one data host is connected. Do not connect a voice device to authenticate on a single-host port. Voice device authorization fails if no voice VLAN is configured on the port.

Multi-domain mode should be configured if data host is connected through an IP phone to the port. Multi-domain mode should be configured if the voice device needs to be authenticated.

Multi-auth mode should be configured to allow devices behind a hub to obtain secured port access through individual authentication. Only one voice device can be authenticated in this mode if a voice VLAN is configured.

Multi-host mode also offers port access for multiple hosts behind a hub, but multi-host mode gives unrestricted port access to the devices after the first user gets authenticated.

Examples

This example shows how to enable multi-auth mode on a port:

```
Controller(config-if)# authentication host-mode multi-auth
```

This example shows how to enable multi-domain mode on a port:

```
Controller(config-if)# authentication host-mode multi-domain
```

This example shows how to enable multi-host mode on a port:

```
Controller(config-if)# authentication host-mode multi-host
```

This example shows how to enable single-host mode on a port:

```
Controller(config-if)# authentication host-mode single-host
```

You can verify your settings by entering the **show authentication sessions interface** *interface* **details** privileged EXEC command.

authentication mac-move permit

To enable MAC move on a controller, use the **authentication mac-move permit** global configuration command. To disable MAC move, use the **no** form of this command.

authentication mac-move permit

no authentication mac-move permit

Syntax Description

This command has no arguments or keywords.

Command Default

MAC move is enabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

This is a legacy command. The new command is **access-session mac-move deny**.

The command enables authenticated hosts to move between any authentication-enabled ports (MAC authentication bypass [MAB], 802.1x, or Web-auth) on a controller. For example, if there is a device between an authenticated host and port, and that host moves to another port, the authentication session is deleted from the first port, and the host is reauthenticated on the new port.

If MAC move is disabled, and an authenticated host moves to another port, it is not reauthenticated, and a violation error occurs.

MAC move is not supported on port-security enabled 802.1x ports. If MAC move is globally configured on the switch and a port security-enabled host moves to an 802.1x-enabled port, a violation error occurs.

Examples

This example shows how to enable MAC move on a controller:

```
Controller(config)# authentication mac-move permit
```

Related Commands

Command	Description
access-session mac-move deny	Disables MAC move on a controller.
authentication event	Sets the action for specific authentication events.

Command	Description
authentication fallback	Configures a port to use web authentication as a fallback method for clients that do not support IEEE 802.1x authentication.
authentication host-mode	Sets the authorization manager mode on a port.
authentication open	Enables or disables open access on a port.
authentication order	Sets the order of authentication methods used on a port.
authentication periodic	Enable or disables reauthentication on a port.
authentication port-control	Enables manual control of the port authorization state.
authentication priority	Adds an authentication method to the port-priority list.
authentication timer	Configures the timeout and reauthentication parameters for an 802.1x-enabled port.
authentication violation	Configures the violation modes that occur when a new device connects to a port or when a new device connects to a port with the maximum number of devices already connected to that port.
show authentication	Displays information about authentication manager events on the switch.

authentication priority

To add an authentication method to the port-priority list, use the **authentication priority** command in interface configuration mode. To return to the default, use the **no** form of this command.

authentication priority [**dot1x** | **mab**] {**webauth**}

no authentication priority [**dot1x** | **mab**] {**webauth**}

Syntax Description

dot1x	(Optional) Adds 802.1x to the order of authentication methods.
mab	(Optional) Adds MAC authentication bypass (MAB) to the order of authentication methods.
webauth	Adds web authentication to the order of authentication methods.

Command Default

The default priority is 802.1x authentication, followed by MAC authentication bypass and web authentication.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Ordering sets the order of methods that the switch attempts when trying to authenticate a new device is connected to a port.

When configuring multiple fallback methods on a port, set web authentication (webauth) last.

Assigning priorities to different authentication methods allows a higher-priority method to interrupt an in-progress authentication method with a lower priority.

Note If a client is already authenticated, it might be reauthenticated if an interruption from a higher-priority method occurs.

The default priority of an authentication method is equivalent to its position in execution-list order: 802.1x authentication, MAC authentication bypass (MAB), and web authentication. Use the **dot1x**, **mab**, and **webauth** keywords to change this default order.

Examples

This example shows how to set 802.1x as the first authentication method and web authentication as the second authentication method:

```
Controller(config-if)# authentication priority dotx webauth
```

This example shows how to set MAB as the first authentication method and web authentication as the second authentication method:

```
Controller(config-if)# authentication priority mab webauth
```

Related Commands

Command	Description
authentication control-direction	Configures the port mode as unidirectional or bidirectional.
authentication event fail	Specifies how the Auth Manager handles authentication failures as a result of unrecognized user credentials.
authentication event no-response action	Specifies how the Auth Manager handles authentication failures as a result of a nonresponsive host.
authentication event server alive action reinitialize	Reinitializes an authorized Auth Manager session when a previously unreachable authentication, authorization, and accounting server becomes available.
authentication event server dead action authorize	Authorizes Auth Manager sessions when the authentication, authorization, and accounting server becomes unreachable.
authentication fallback	Enables a web authentication fallback method.
authentication host-mode	Allows hosts to gain access to a controlled port.
authentication open	Enables open access on a port.
authentication order	Specifies the order in which the Auth Manager attempts to authenticate a client on a port.
authentication periodic	Enables automatic reauthentication on a port.
authentication port-control	Configures the authorization state of a controlled port.
authentication timer inactivity	Configures the time after which an inactive Auth Manager session is terminated.
authentication timer reauthenticate	Specifies the period of time between which the Auth Manager attempts to reauthenticate authorized ports.

Command	Description
authentication timer restart	Specifies the period of time after which the Auth Manager attempts to authenticate an unauthorized port.
authentication violation	Specifies the action to be taken when a security violation occurs on a port.
mab	Enables MAC authentication bypass on a port.
show authentication registrations	Displays information about the authentication methods that are registered with the Auth Manager.
show authentication sessions	Displays information about current Auth Manager sessions.
show authentication sessions interface	Displays information about the Auth Manager for a given interface.

authentication violation

To configure the violation modes that occur when a new device connects to a port or when a new device connects to a port after the maximum number of devices are connected to that port, use the **authentication violation** interface configuration command.

authentication violation { **protect**|**replace**|**restrict**|**shutdown** }

no authentication violation { **protect**|**replace**|**restrict**|**shutdown** }

Syntax Description

protect	Drops unexpected incoming MAC addresses. No syslog errors are generated.
replace	Removes the current session and initiates authentication with the new host.
restrict	Generates a syslog error when a violation error occurs.
shutdown	Error-disables the port or the virtual port on which an unexpected MAC address occurs.

Command Default

authentication violation shutdown mode is enabled.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Use the **authentication violation** command to specify the action to be taken when a security violation occurs on a port.

Examples

This example shows how to configure an IEEE 802.1x-enabled port as error-disabled and to shut down when a new device connects it:

```
Controller(config-if)# authentication violation shutdown
```

This example shows how to configure an 802.1x-enabled port to generate a system error message and to change the port to restricted mode when a new device connects to it:

```
Controller(config-if)# authentication violation restrict
```

This example shows how to configure an 802.1x-enabled port to ignore a new device when it connects to the port:

```
Controller(config-if)# authentication violation protect
```

This example shows how to configure an 802.1x-enabled port to remove the current session and initiate authentication with a new device when it connects to the port:

```
Controller(config-if)# authentication violation replace
```

You can verify your settings by entering the **show authentication** privileged EXEC command.

cisp enable

To enable Client Information Signaling Protocol (CISP) on a switch so that it acts as an authenticator to a supplicant switch, use the **cisp enable** global configuration command.

cisp enable

no cisp enable

Syntax Description

This command has no arguments or keywords.

Command Default

There is no default setting.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The link between the authenticator and supplicant switch is a trunk. When you enable VTP on both switches, the VTP domain name must be the same, and the VTP mode must be server.

To avoid the MD5 checksum mismatch error when you configure VTP mode, verify that:

- VLANs are not configured on two different switches, which can be caused by two VTP servers in the same domain.
- Both switches have different configuration revision numbers.

Examples

This example shows how to enable CISP:

```
Controller(config)# cisp enable
```

Related Commands

Command	Description
dot1x credentials*profile*	Configures a profile on a supplicant switch.
dot1x supplicant force-multicast	Forces 802.1X supplicant to send multicast packets.
dot1x supplicant controlled transient	Configures controlled access by 802.1X supplicant.
show cisp	Displays CISP information for a specified interface.

clear errdisable interface vlan

To reenable a VLAN that was error-disabled, use the **clear errdisable interface** privileged EXEC command on the switch.

clear errdisable interface *interface-id* **vlan** [*vlan-list*]

Syntax Description

interface-id	Specify an interface.
vlan list	(Optional) Specifies a list of VLANs to be reenabled. If a VLAN list is not specified, then all VLANs are reenabled.

Command Default

No default is defined.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You can reenable a port by using the **shutdown** and **no shutdown** interface configuration commands, or you can clear error-disable for VLANs by using the **clear errdisable** interface command.

Examples

This example shows how to reenable all VLANs that were error-disabled on Gigabit Ethernet port 4/0/2:

```
Controller# clear errdisable interface gigabitethernet4/0/2 vlan
```

Related Commands

Command	Description
errdisable detect cause	Enables error-disabled detection for a specific cause or all causes.
errdisable recovery	Configures the recovery mechanism variables.
show errdisable detect	Displays error-disabled detection status.
show errdisable recovery	Displays error-disabled recovery timer information.

Command	Description
show interfaces status err-disabled	Displays interface status of a list of interfaces in error-disabled state.

clear mac address-table

To delete from the MAC address table a specific dynamic address, all dynamic addresses on a particular interface, all dynamic addresses on stack members, or all dynamic addresses on a particular VLAN, use the **clear mac address-table** command in privileged EXEC mode. This command also clears the MAC address notification global counters.

clear mac address-table {**dynamic** [**address** *mac-addr* | **interface** *interface-id* | **vlan** *vlan-id*] | **move update** | **notification**}

Syntax Description

dynamic	Deletes all dynamic MAC addresses.
address *mac-addr*	(Optional) Deletes the specified dynamic MAC address.
interface *interface-id*	(Optional) Deletes all dynamic MAC addresses on the specified physical port or port channel.
vlan *vlan-id*	(Optional) Deletes all dynamic MAC addresses for the specified VLAN. The range is 1 to 4094.
move update	Clears the MAC address table move-update counters.
notification	Clears the notifications in the history table and reset the counters.

Command Default

No default is defined.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You can verify that the information was deleted by entering the **show mac address-table** privileged EXEC command.

Examples

This example shows how to remove a specific MAC address from the dynamic address table:

```
Controller# clear mac address-table dynamic address 0008.0070.0007
```

Related Commands

Command	Description
mac address-table notification	Enables the MAC address notification feature.
mac address-table move update {**receive** | **transmit**}	Configures MAC address-table move update on the switch.
show mac address-table	Displays the MAC address table static and dynamic entries.
show mac address-table move update	Displays the MAC address-table move update information on the switch.
show mac address-table notification	Displays the MAC address notification settings for all interfaces or on the specified interface when the **interface** keyword is appended.
snmp trap mac-notification change	Enables the SNMP MAC address notification trap on a specific interface.

deny (MAC access-list configuration)

To prevent non-IP traffic from being forwarded if the conditions are matched, use the **deny** MAC access-list configuration command on the switch stack or on a standalone switch. To remove a deny condition from the named MAC access list, use the **no** form of this command.

deny {**any** | **host** *src-MAC-addr* | *src-MAC-addr mask*} {**any** | **host** *dst-MAC-addr* | *dst-MAC-addr mask*} [*type mask* | **aarp** | **amber** | **appletalk** | **dec-spanning** | **decnet-iv** | **diagnostic** | **dsm** | **etype-6000** | **etype-8042** | **lat** | **lavc-sca** | **lsap** *lsap mask* | **mop-console** | **mop-dump** | **msdos** | **mumps** | **netbios** | **vines-echo** | **vines-ip** | **xns-idp**][**cos** *cos*]

no deny {**any** | **host** *src-MAC-addr* | *src-MAC-addr mask*} {**any** | **host** *dst-MAC-addr* | *dst-MAC-addr mask*} [*type mask* | **aarp** | **amber** | **appletalk** | **dec-spanning** | **decnet-iv** | **diagnostic** | **dsm** | **etype-6000** | **etype-8042** | **lat** | **lavc-sca** | **lsap** *lsap mask* | **mop-console** | **mop-dump** | **msdos** | **mumps** | **netbios** | **vines-echo** | **vines-ip** | **xns-idp**][**cos** *cos*]

Syntax Description

any	Denies any source or destination MAC address.
host *src-MAC-addr* | *src-MAC-addr mask*	Defines a host MAC address and optional subnet mask. If the source address for a packet matches the defined address, non-IP traffic from that address is denied.
host *dst-MAC-addr* | *dst-MAC-addr mask*	Defines a destination MAC address and optional subnet mask. If the destination address for a packet matches the defined address, non-IP traffic to that address is denied.
type mask	(Optional) Specifies the Ethertype number of a packet with Ethernet II or SNAP encapsulation to identify the protocol of the packet. The type is 0 to 65535, specified in hexadecimal. The mask is a mask of don't care bits applied to the Ethertype before testing for a match.
aarp	(Optional) Specifies Ethertype AppleTalk Address Resolution Protocol that maps a data-link address to a network address.
amber	(Optional) Specifies EtherType DEC-Amber.
appletalk	(Optional) Specifies EtherType AppleTalk/EtherTalk.
dec-spanning	(Optional) Specifies EtherType Digital Equipment Corporation (DEC) spanning tree.
decnet-iv	(Optional) Specifies EtherType DECnet Phase IV protocol.
diagnostic	(Optional) Specifies EtherType DEC-Diagnostic.
dsm	(Optional) Specifies EtherType DEC-DSM.

etype-6000	(Optional) Specifies EtherType 0x6000.
etype-8042	(Optional) Specifies EtherType 0x8042.
lat	(Optional) Specifies EtherType DEC-LAT.
lavc-sca	(Optional) Specifies EtherType DEC-LAVC-SCA.
lsap *lsap-number mask*	(Optional) Specifies the LSAP number (0 to 65535) of a packet with 802.2 encapsulation to identify the protocol of the packet. *mask* is a mask of don't care bits applied to the LSAP number before testing for a match.
mop-console	(Optional) Specifies EtherType DEC-MOP Remote Console.
mop-dump	(Optional) Specifies EtherType DEC-MOP Dump.
msdos	(Optional) Specifies EtherType DEC-MSDOS.
mumps	(Optional) Specifies EtherType DEC-MUMPS.
netbios	(Optional) Specifies EtherType DEC- Network Basic Input/Output System (NETBIOS).
vines-echo	(Optional) Specifies EtherType Virtual Integrated Network Service (VINES) Echo from Banyan Systems.
vines-ip	(Optional) Specifies EtherType VINES IP.
xns-idp	(Optional) Specifies EtherType Xerox Network Systems (XNS) protocol suite (0 to 65535), an arbitrary Ethertype in decimal, hexadecimal, or octal.
cos *cos*	(Optional) Specifies a class of service (CoS) number from 0 to 7 to set priority. Filtering on CoS can be performed only in hardware. A warning message reminds the user if the **cos** option is configured.

Command Default

This command has no defaults. However, the default action for a MAC-named ACL is to deny.

Command Modes

MAC-access list configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You enter MAC-access list configuration mode by using the **mac access-list extended** global configuration command.

If you use the **host** keyword, you cannot enter an address mask; if you do not use the **host** keyword, you must enter an address mask.

When an access control entry (ACE) is added to an access control list, an implied **deny-any-any** condition exists at the end of the list. That is, if there are no matches, the packets are denied. However, before the first ACE is added, the list permits all packets.

To filter IPX traffic, you use the *type mask* or **lsap** *lsap mask* keywords, depending on the type of IPX encapsulation being used. Filter criteria for IPX encapsulation types as specified in Novell terminology and Cisco IOS terminology are listed in the table.

Table 11: IPX Filtering Criteria

IPX Encapsulation Type		Filter Criterion
Cisco IOS Name	**Novel Name**	
arpa	Ethernet II	Ethertype 0x8137
snap	Ethernet-snap	Ethertype 0x8137
sap	Ethernet 802.2	LSAP 0xE0E0
novell-ether	Ethernet 802.3	LSAP 0xFFFF

Examples

This example shows how to define the named MAC extended access list to deny NETBIOS traffic from any source to MAC address 00c0.00a0.03fa. Traffic matching this list is denied.

```
Controller(config-ext-macl)# deny any host 00c0.00a0.03fa netbios.
```

This example shows how to remove the deny condition from the named MAC extended access list:

```
Controller(config-ext-macl)# no deny any 00c0.00a0.03fa 0000.0000.0000 netbios.
```

This example denies all packets with Ethertype 0x4321:

```
Controller(config-ext-macl)# deny any any 0x4321 0
```

You can verify your settings by entering the **show access-lists** privileged EXEC command.

Related Commands

Command	Description
mac access-list extended	Creates an access list based on MAC addresses for non-IP traffic.

Command	Description
permit	Permits from the MAC access-list configuration. Permits non-IP traffic to be forwarded if conditions are matched.
show access-lists	Displays access control lists configured on a switch.

device-role (IPv6 snooping)

To specify the role of the device attached to the port, use the **device-role** command in IPv6 snooping configuration mode.

device-role {**node** | **switch**}

Syntax Description

node	Sets the role of the attached device to node.
switch	Sets the role of the attached device to switch.

Command Default

The device role is node.

Command Modes

IPv6 snooping configuration (config-ipv6-snooping)

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The **device-role** command specifies the role of the device attached to the port. By default, the device role is node.

The **switch** keyword indicates that the remote device is a switch and that the local switch is now operating in multiswitch mode; binding entries learned from the port will be marked with trunk_port preference level. If the port is configured as a trust-port, binding entries will be marked with trunk_trusted_port preference level.

Examples

This example shows how to define an IPv6 snooping policy name as policy1, place the device in IPv6 snooping configuration mode, and configure the device as the node:

```
Controller(config)# ipv6 snooping policy policy1
Controller(config-ipv6-snooping)# device-role node
```

device-role (IPv6 nd inspection)

Use the **device-role** command in neighbor discovery (ND) inspection policy configuration mode to specify the role of the device attached to the port.

device-role {**host** | **monitor** | **router** | **switch**}

Syntax Description

host	Sets the role of the attached device to host.
monitor	Sets the role of the attached device to monitor.
router	Sets the role of the attached device to router.
switch	Sets the role of the attached device to switch.

Command Default

The device role is host.

Command Modes

ND inspection policy configuration (config-nd-inspection)

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The **device-role** command specifies the role of the device attached to the port. By default, the device role is host, and therefore all the inbound router advertisement and redirect messages are blocked. If the device role is enabled using the **router** keyword, all messages (router solicitation [RS], router advertisement [RA], or redirect) are allowed on this port.

When the **router** or **monitor** keyword is used, the multicast RS messages are bridged on the port, regardless of whether limited broadcast is enabled. However, the monitor keyword does not allow inbound RA or redirect messages. When the monitor keyword is used, devices that need these messages will receive them.

The **switch** keyword indicates that the remote device is a switch and that the local switch is now operating in multiswitch mode; binding entries learned from the port will be marked with trunk_port preference level. If the port is configured as a trust-port, binding entries will be marked with trunk_trusted_port preference level.

Examples

The following example defines a Neighbor Discovery Protocol (NDP) policy name as policy1, places the device in ND inspection policy configuration mode, and configures the device as the host:

```
Controller(config)#  ipv6 nd inspection policy policy1
Controller(config-nd-inspection)# device-role host
```

dot1x critical (global configuration)

To configure the IEEE 802.1X critical authentication parameters, use the **dot1x critical** command in global configuration mode.

dot1x critical eapol

Syntax Description

eapol	Specifies that the switch send an EAPOL-Success message when the switch successfully authenticates the critical port.

Command Default

eapol is disabled

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Examples

This example shows how to specify that the switch sends an EAPOL-Success message when the switch successfully authenticates the critical port:

```
Controller(config)# dot1x critical eapol
```

dot1x max-start

To set the maximum number of Extensible Authentication Protocol over LAN (EAPOL) start frames that a supplicant sends (assuming that no response is received) to the client before concluding that the other end is 802.1X unaware, use the **dot1x max-start** command in interface configuration mode. To remove the maximum number-of-times setting, use the **no** form of this command.

dot1x max-start *number*

no dot1x max-start

Syntax Description

number	Maximum number of times that the router sends an EAPOL start frame. The value is from 1 to 10. The default is 3.

Command Default

The default maximum number setting is 3.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You must enter the **switchport mode access** interface configuration command on a switch port before entering this command.

Examples

The following example shows that the maximum number of EAPOL Start requests has been set to 5:

```
Controller(config)# interface g1/0/3
Controller(config-if)# dot1x max-start 5
```

dot1x pae

To set the Port Access Entity (PAE) type, use the **dot1x pae** command in interface configuration mode. To disable the PAE type that was set, use the **no** form of this command.

dot1x pae {**supplicant** | **authenticator**}

no dot1x pae {**supplicant** | **authenticator**}

Syntax Description

supplicant	The interface acts only as a supplicant and will not respond to messages that are meant for an authenticator.
authenticator	The interface acts only as an authenticator and will not respond to any messages meant for a supplicant.

Command Default

PAE type is not set.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Use the **no dot1x pae** interface configuration command to disable IEEE 802.1x authentication on the port.

When you configure IEEE 802.1x authentication on a port, such as by entering the **dot1x port-control** interface configuration command, the switch automatically configures the port as an IEEE 802.1x authenticator. After the **no dot1x pae** interface configuration command is entered, the Authenticator PAE operation is disabled.

Examples

The following example shows that the interface has been set to act as a supplicant:

```
Controller(config)# interface g1/0/3
Controller(config-if)# dot1x pae supplicant
```

dot1x supplicant force-multicast

To force a supplicant switch to send only multicast Extensible Authentication Protocol over LAN (EAPOL) packets whenever it receives multicast or unicast EAPOL packets, use the **dot1x supplicant force-multicast** global configuration command. To return to the default setting, use the **no** form of this command.

dot1x supplicant force-multicast

no dot1x supplicant force-multicast

Syntax Description

This command has no arguments or keywords.

Command Default

The supplicant switch sends unicast EAPOL packets when it receives unicast EAPOL packets. Similarly, it sends multicast EAPOL packets when it receives multicast EAPOL packets.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Enable this command on the supplicant switch for Network Edge Access Topology (NEAT) to work in all host modes.

Examples

This example shows how force a supplicant switch to send multicast EAPOL packets to the authenticator switch:

```
Controller(config)# dot1x supplicant force-multicast
```

Related Commands

Command	Description
cisp enable	Enable Client Information Signalling Protocol (CISP) on a switch so that it acts as an authenticator to a supplicant switch.
dot1x credentials	Configure the 802.1x supplicant credentials on the port.
dot1x pae supplicant	Configure an interface to act only as a supplicant.

dot1x test eapol-capable

To monitor IEEE 802.1x activity on all the switch ports and to display information about the devices that are connected to the ports that support IEEE 802.1x, use the **dot1x test eapol-capable** privileged EXEC command on the switch stack or on a standalone switch.

dot1x test eapol-capable [**interface** *interface-id*]

Syntax Description

interface *interface-id*	(Optional) Port to be queried.

Command Default

There is no default setting.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Use this command to test the IEEE 802.1x capability of the devices connected to all ports or to specific ports on a switch.

There is not a no form of this command.

Examples

This example shows how to enable the IEEE 802.1x readiness check on a switch to query a port. It also shows the response received from the queried port verifying that the device connected to it is IEEE 802.1x-capable:

```
Controller# dot1x test eapol-capable interface gigabitethernet1/0/13

DOT1X_PORT_EAPOL_CAPABLE:DOT1X: MAC 00-01-02-4b-f1-a3 on gigabitethernet1/0/13 is EAPOL
capable
```

Related Commands

Command	Description
dot1x test timeout *timeout*	Configures the timeout used to wait for EAPOL response to an IEEE 802.1x readiness query.

dot1x test timeout

To configure the timeout used to wait for EAPOL response from a port being queried for IEEE 802.1x readiness, use the **dot1x test timeout** global configuration command on the switch stack or on a standalone switch.

dot1x test timeout *timeout*

Syntax Description

timeout	Time in seconds to wait for an EAPOL response. The range is from 1 to 65535 seconds.

Command Default

The default setting is 10 seconds.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Use this command to configure the timeout used to wait for EAPOL response.

There is not a no form of this command.

Examples

This example shows how to configure the switch to wait 27 seconds for an EAPOL response:

```
Controller# dot1x test timeout 27
```

You can verify the timeout configuration status by entering the **show run** privileged EXEC command.

Related Commands

Command	Description
dot1x test eapol-capable [**interface** *interface-id*]	Checks for IEEE 802.1x readiness on devices connected to all or to specified IEEE 802.1x-capable ports.

dot1x timeout

To configure the value for retry timeouts, use the **dot1x timeout** command in global configuration or interface configuration mode. To return to the default value for retry timeouts, use the **no** form of this command.

dot1x timeout {**auth-period** *seconds* | **held-period** *seconds* | **quiet-period** *seconds* | **ratelimit-period** *seconds* | **server-timeout** *seconds* | **start-period** *seconds* | **supp-timeout** *seconds* | **tx-period** *seconds*}

Syntax Description

auth-period *seconds*	Configures the time, in seconds for which a supplicant will stay in the HELD state (that is, the length of time it will wait before trying to send the credentials again after a failed attempt). The range is from 1 to 65535. The default is 30.
held-period *seconds*	Configures the time, in seconds for which a supplicant will stay in the HELD state (that is, the length of time it will wait before trying to send the credentials again after a failed attempt). The range is from 1 to 65535. The default is 60
quiet-period *seconds*	Configures the time, in seconds, that the authenticator (server) remains quiet (in the HELD state) following a failed authentication exchange before trying to reauthenticate the client. The range is from 1 to 65535. The default is 60
ratelimit-period *seconds*	Throttles the EAP-START packets that are sent from misbehaving client PCs (for example, PCs that send EAP-START packets that result in the wasting of switch processing power). • The authenticator ignores EAPOL-Start packets from clients that have successfully authenticated for the rate-limit period duration. • The range is from 1 to 65535. By default, rate limiting is disabled.
server-timeout *seconds*	Configures the interval, in seconds, between two successive EAPOL-Start frames when they are being retransmitted. • The range is from 1 to 65535. The default is 30. If the server does not send a response to an 802.1X packet within the specified period, the packet is sent again.
start-period *seconds*	Configures the interval, in seconds, between two successive EAPOL-Start frames when they are being retransmitted. The range is from 1 to 65535. The default is 30.

supp-timeout *seconds*	Sets the authenticator-to-supplicant retransmission time for all EAP messages other than EAP Request ID. The range is from 1 to 65535. The default is 30.
tx-period *seconds*	Configures the number of seconds between retransmission of EAP request ID packets (assuming that no response is received) to the client. • The range is from 1 to 65535. The default is 30. • If an 802.1X packet is sent to the supplicant and the supplicant does not send a response after the retry period, the packet will be sent again.

Command Default

Periodic reauthentication and periodic rate-limiting are done.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You should change the default value of this command only to adjust for unusual circumstances such as unreliable links or specific behavioral problems with certain clients and authentication servers.

The **dot1x timeout reauth-period** interface configuration command affects the behavior of the switch only if you have enabled periodic re-authentication by using the **dot1x reauthentication** interface configuration command.

During the quiet period, the switch does not accept or initiate any authentication requests. If you want to provide a faster response time to the user, enter a number smaller than the default.

When the **ratelimit-period** is set to 0 (the default), the switch does not ignore EAPOL packets from clients that have been successfully authenticated and forwards them to the RADIUS server.

Examples

The following example shows that various 802.1X retransmission and timeout periods have been set:

```
Controller(config)# configure terminal
Controller(config)# interface g1/0/3
Controller(config-if)# dot1x port-control auto
Controller(config-if)# dot1x timeout auth-period 2000
Controller(config-if)# dot1x timeout held-period 2400
Controller(config-if)# dot1x timeout quiet-period 600
Controller(config-if)# dot1x timeout start-period 90
Controller(config-if)# dot1x timeout supp-timeout 300
Controller(config-if)# dot1x timeout tx-period 60
```

```
Controller(config-if)# dot1x timeout server-timeout 60
```

epm access-control open

To configure an open directive for ports that do not have an access control list (ACL) configured, use the **epm access-control open** command in global configuration mode. To disable the open directive, use the **no** form of this command.

epm access-control open

no epm access-control open

Syntax Description

This command has no arguments or keywords.

Command Default

The default directive applies.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Use this command to configure an open directive that allows hosts without an authorization policy to access ports configured with a static ACL. If you do not configure this command, the port applies the policies of the configured ACL to the traffic. If no static ACL is configured on a port, both the default and open directives allow access to the port.

You can verify your settings by entering the **show running-config** privileged EXEC command.

Examples

This example shows how to configure an open directive.

```
Controller(config)# epm access-control open
```

Related Commands

Command	Description
show running-config	Displays the contents of the current running configuration file.

ip admission

Use the **ip admission** configuration command to enable web authentication. You can also use this command in fallback-profile mode. Use the **no** form of this command to disable web authentication.

ip admission *rule*

no ip admission *rule*

Syntax Description

rule	IP admission rule name.

Command Default

Web authentication is disabled.

Command Modes

Interface configuration

Fallback-profile mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The **ip admission** command applies a web authentication rule to a switch port.

Examples

This example shows how to apply a web authentication rule to a switchport:

```
Controller# configure terminal
Controller(config)# interface gigabitethernet1/0/1
Controller(config-if)# ip admission rule1
```

This example shows how to apply a web authentication rule to a fallback profile for use on an IEEE 802.1x enabled switch port.

```
Controller# configure terminal
Controller(config)# fallback profile profile1
Controller(config-fallback-profile)# ip admission rule1
```

ip admission name

To enable web authentication, use the **ip admission name** command in global configuration mode. To disable web authentication, use the **no** form of this command.

ip admission name *name* {**consent** | **proxy http**} [**absolute timer** *minutes* | **inactivity-time** *minutes* | **list** {*acl* | *acl-name*} | **service-policy type tag** *service-policy-name*]

no ip admission name *name* {**consent** | **proxy http**} [**absolute timer** *minutes* | **inactivity-time** *minutes* | **list** {*acl* | *acl-name*} | **service-policy type tag** *service-policy-name*]

Syntax Description

name	Name of network admission control rule.
consent	Associates an authentication proxy consent web page with the IP admission rule specified using the *admission-name* argument.
proxy http	Configures web authentication custom page.
absolute-timer *minutes*	(Optional) Elapsed time, in minutes, before the external server times out.
inactivity-time *minutes*	(Optional) Elapsed time, in minutes, before the external file server is deemed unreachable.
list	(Optional) Associates the named rule with an access control list (ACL).
acl	Applies a standard, extended list to a named admission control rule. The value ranges from 1 through 199, or from 1300 through 2699 for expanded range.
acl-name	Applies a named access list to a named admission control rule.
service-policy type tag	(Optional) A control plane service policy is to be configured.
service-policy-name	Control plane tag service policy that is configured using the **policy-map type control tag***policyname* command, keyword, and argument. This policy map is used to apply the actions on the host when a tag is received.

Command Default

Web authentication is disabled.

Command Modes Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines The **ip admission name** command globally enables web authentication on a switch.

After you enable web authentication on a switch, use the **ip access-group in** and **ip admission web-rule** interface configuration commands to enable web authentication on a specific interface.

Examples This example shows how to configure only web authentication on a switch port:

```
Controller# configure terminal
Controller(config) ip admission name http-rule proxy http
Controller(config)# interface gigabitethernet1/0/1
Controller(config-if)# ip access-group 101 in
Controller(config-if)# ip admission rule
Controller(config-if)# end
```

This example shows how to configure IEEE 802.1x authentication with web authentication as a fallback mechanism on a switch port:

```
Controller# configure terminal
Controller(config)# ip admission name rule2 proxy http
Controller(config)# fallback profile profile1
Controller(config)# ip access group 101 in
Controller(config)# ip admission name rule2
Controller(config)# interface gigabitethernet1/0/1
Controller(config-if)# dot1x port-control auto
Controller(config-if)# dot1x fallback profile1
Controller(config-if)# end
```

Related Commands

Command	Description
dot1x fallback	Configures a port to use web authentication as a fallback method for clients that do not support IEEE 802.1x authentication.
fallback profile	Creates a web authentication fallback profile.
ip admission	Enables web authentication on a port.
show authentication sessions interface *interface* **detail**	Displays information about the web authentication session status.

Command	Description
show ip admission	Displays information about NAC cached entries or the NAC configuration.

ip device tracking maximum

To enable IP port security binding tracking on a Layer 2 port, use the **ip device tracking maximum** command in interface configuration mode. To disable IP port security on untrusted Layer 2 interfaces, use the **no** form of this command.

ip device tracking maximum *number*

no ip device tracking maximum *number*

Syntax Description

number	Number of bindings created in the IP device tracking table for a port. The range is 1 to 10.

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to enable IP port security with IP-MAC filters on a Layer 2 access port:

```
Controller# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)# ip device tracking
Controller(config)# interface gigabitethernet1/0/3
Controller(config-if)# switchport mode access
Controller(config-if)# switchport access vlan 1
Controller(config-if)# ip device tracking maximum 5
Controller(config-if)# switchport port-security
Controller(config-if)# switchport port-security maximum 5
Controller(config-if)# end
```

ip device tracking probe

To configure the IP device tracking table for Address Resolution Protocol (ARP) probes, use the **ip device tracking probe** command in global configuration mode. To disable ARP probes, use the **no** form of this command.

ip device tracking probe {**count** *number*| **delay** *seconds*| **interval** *seconds*| **use-svi** *address*}

no ip device tracking probe {**count** *number*| **delay** *seconds*| **interval** *seconds*| **use-svi** *address*}

Syntax Description

count *number*	Sets the number of times that the controller sends the ARP probe. The range is from 1 to 255.
delay *seconds*	Sets the number of seconds that the controller waits before sending the ARP probe. The range is from 1 to 120.
interval *seconds*	Sets the number of seconds that the controller waits for a response before resending the ARP probe. The range is from 30 to 1814400 seconds.
use-svi	Uses the controller virtual interface (SVI) IP address as source of ARP probes.

Command Default

The count number is 3.

There is no delay.

The interval is 30 seconds.

The ARP probe default source IP address is the Layer 3 interface and 0.0.0.0 for switchports.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Use the **use-svi** keyword to configure the IP device tracking table to use the SVI IP address for ARP probes in cases when the default source IP address 0.0.0.0 for switch ports is used and the ARP probes drop.

Examples

This example shows how to set SVI as the source for ARP probes:

```
Controller(config)# ip device tracking probe use-svi
```

ip dhcp snooping database

To configure the Dynamic Host Configuration Protocol (DHCP)-snooping database, use the **ip dhcp snooping database** command in global configuration mode. To disable the DHCP-snooping database, use the **no** form of this command.

ip dhcp snooping database {**crashinfo:***url* | **flash:***url* | **ftp:***url* | **http:***url* | **https:***url* | **rcp:***url* | **scp:***url* | **tftp:***url* | **timeout** *seconds* | **usbflash0:***url* | **write-delay** *seconds*}

Syntax Description

crashinfo:*url*	Specifies the database URL for storing entries using crashinfo.
flash:*url*	Specifies the database URL for storing entries using flash.
ftp:*url*	Specifies the database URL for storing entries using FTP.
http:*url*	Specifies the database URL for storing entries using HTTP.
https:*url*	Specifies the database URL for storing entries using secure HTTP (https).
rcp:*url*	Specifies the database URL for storing entries using remote copy (rcp).
scp:*url*	Specifies the database URL for storing entries using Secure Copy (SCP).
tftp:*url*	Specifies the database URL for storing entries using TFTP.
timeout *seconds*	Specifies the abort timeout interval; valid values are from 0 to 86400 seconds.
usbflash0:*url*	Specifies the database URL for storing entries using USB flash.
write-delay: *seconds*	Specifies the amount of time before writing the DHCP-snooping entries to an external server after a change is seen in the local DHCP-snooping database; valid values are from 15 to 86400 seconds.

Command Default

The DHCP-snooping database is not configured.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You must enable DHCP snooping on the interface before entering this command. Use the **ip dhcp snooping** command to enable DHCP snooping.

Examples

This example shows how to specify the database URL using TFTP:

```
Controller(config)#  ip dhcp snooping database tftp://10.90.90.90/snooping-rp2
```

This example shows how to specify the amount of time before writing DHCP snooping entries to an external server:

```
Controller(config)#  ip dhcp snooping database write-delay 15
```

ip dhcp snooping information option format remote-id

To configure the option-82 remote-ID suboption, use the **ip dhcp snooping information option format remote-id** global configuration command on the switch to configure the option-82 remote-ID suboption. Use the **no** form of this command to configure the default remote-ID suboption.

ip dhcp snooping information option format remote-id {**hostname** | **string** *string*}

no ip dhcp snooping information option format remote-id {**hostname** | **string** *string*}

Syntax Description

hostname	Specify the switch hostname as the remote ID.
string *string*	Specify a remote ID, using from 1 to 63 ASCII characters (no spaces).

Command Default

The switch MAC address is the remote ID.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You must globally enable DHCP snooping by using the **ip dhcp snooping** global configuration command for any DHCP snooping configuration to take effect.

When the option-82 feature is enabled, the default remote-ID suboption is the switch MAC address. This command allows you to configure either the switch hostname or a string of up to 63 ASCII characters (but no spaces) to be the remote ID.

Note If the hostname exceeds 63 characters, it will be truncated to 63 characters in the remote-ID configuration.

Examples

This example shows how to configure the option- 82 remote-ID suboption:

```
Controller(config)# ip dhcp snooping information option format remote-id hostname
```

ip dhcp snooping verify no-relay-agent-address

To disable the DHCP snooping feature from verifying that the relay agent address (giaddr) in a DHCP client message matches the client hardware address on an untrusted port, use the **ip dhcp snooping verify no-relay-agent-address** command in global configuration mode. To enable verification, use the **no** form of this command.

ip dhcp snooping verify no-relay-agent-address

no ip dhcp snooping verify no-relay-agent-address

Syntax Description

This command has no arguments or keywords.

Command Default

The DHCP snooping feature verifies that the relay-agent IP address (giaddr) field in DHCP client message on an untrusted port is 0.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

By default, the DHCP snooping feature verifies that the relay-agent IP address (giaddr) field in DHCP client message on an untrusted port is 0; the message is dropped if the giaddr field is not 0. Use the **ip dhcp snooping verify no-relay-agent-address** command to disable the verification. Use the **no ip dhcp snooping verify no-relay-agent-address** to reenable verification.

Examples

This example shows how to enable verification of the giaddr in a DHCP client message:

```
Controller(config)# no ip dhcp snooping verify no-relay-agent-address
```

ip source binding

To add a static IP source binding entry, use the **ip source binding** command. Use the **no** form of this command to delete a static IP source binding entry

ip source binding *mac-address* **vlan** *vlan-id ip-address* **interface** *interface-id*

no ip source binding *mac-address* **vlan** *vlan-id ip-address* **interface** *interface-id*

Syntax Description

mac-address	Binding MAC address.
vlan *vlan-id*	Specifies the Layer 2 VLAN identification; valid values are from 1 to 4094.
ip-address	Binding IP address.
interface *interface-id*	ID of the physical interface.

Command Default

No IP source bindings are configured.

Command Modes

Global configuration.

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You can use this command to add a static IP source binding entry only.

The **no** format deletes the corresponding IP source binding entry. It requires the exact match of all required parameter in order for the deletion to be successful. Note that each static IP binding entry is keyed by a MAC address and a VLAN number. If the command contains the existing MAC address and VLAN number, the existing binding entry is updated with the new parameters instead of creating a separate binding entry.

Examples

This example shows how to add a static IP source binding entry:

```
Controller# configure terminal
Controllerconfig) ip source binding 0100.0230.0002 vlan 11 10.0.0.4 interface
gigabitethernet1/0/1
```

ip verify source

To enable IP source guard on an interface, use the **ip verify source** command in interface configuration mode. To disable IP source guard, use the **no** form of this command.

ip verify source [**mac-check**]

no ip verify source [**mac-check**]

Syntax Description

mac-check	(Optional) Enables IP source guard with MAC address verification.

Command Default

IP source guard is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

To enable IP source guard with source IP address filtering, use the **ip verify source** interface configuration command.

To enable IP source guard with source IP address filtering and MAC address verification, use the **ip verify source mac-check** interface configuration command.

Examples

This example shows how to enable IP source guard with source IP address filtering on an interface:

```
Controller(config-if)# ip verify source
```

This example shows how to enable IP source guard with source IP address filtering and MAC address verification:

```
Controller(config-if)# ip verify source mac-check
```

You can verify your settings by entering the **show ip verify source** privileged EXEC command.

ipv6 snooping policy

To configure an IPv6 snooping policy and enter IPv6 snooping configuration mode, use the **ipv6 snooping policy** command in global configuration mode. To delete an IPv6 snooping policy, use the **no** form of this command.

ipv6 snooping policy *snooping-policy*

no ipv6 snooping policy *snooping-policy*

Syntax Description

snooping-policy	User-defined name of the snooping policy. The policy name can be a symbolic string (such as Engineering) or an integer (such as 0).

Command Default

An IPv6 snooping policy is not configured.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Use the **ipv6 snooping policy** command to create an IPv6 snooping policy. When the **ipv6 snooping policy** command is enabled, the configuration mode changes to IPv6 snooping configuration mode. In this mode, the administrator can configure the following IPv6 first-hop security commands:

- The **device-role** command specifies the role of the device attached to the port.
- The **limit address-count** *maximum* command limits the number of IPv6 addresses allowed to be used on the port.
- The **protocol** command specifies that addresses should be gleaned with Dynamic Host Configuration Protocol (DHCP) or Neighbor Discovery Protocol (NDP).
- The **security-level** command specifies the level of security enforced.
- The **tracking** command overrides the default tracking policy on a port.
- The **trusted-port** command configures a port to become a trusted port; that is, limited or no verification is performed when messages are received.

Examples

This example shows how to configure an IPv6 snooping policy:

```
Controller(config)# ipv6 snooping policy policy1
```

```
Controller(config-ipv6-snooping)#
```

limit address-count

To limit the number of IPv6 addresses allowed to be used on the port, use the **limit address-count** command in Neighbor Discovery Protocol (NDP) inspection policy configuration mode or IPv6 snooping configuration mode. To return to the default, use the **no** form of this command.

limit address-count *maximum*

no limit address-count

Syntax Description

maximum	The number of addresses allowed on the port. The range is from 1 to 10000.

Command Default

The default is no limit.

Command Modes

ND inspection policy configuration (config-nd-inspection)

IPv6 snooping configuration (ipv6-snooping)

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The **limit address-count** command limits the number of IPv6 addresses allowed to be used on the port on which the policy is applied. Limiting the number of IPv6 addresses on a port helps limit the binding table size. The range is from 1 to 10000.

Examples

This example shows how to define an NDP policy name as policy1, place the switch in NDP inspection policy configuration mode, and limit the number of IPv6 addresses allowed on the port to 25:

```
Controller(config)# ipv6 nd inspection policy policy1
Controller(config-nd-inspection)# limit address-count 25
```

This example shows how to define an IPv6 snooping policy name as policy1, place the switch in IPv6 snooping policy configuration mode, and limit the number of IPv6 addresses allowed on the port to 25:

```
Controller(config)# ipv6 snooping policy policy1
Controller(config-ipv6-snooping)# limit address-count 25
```

mab request format attribute 32

To enable VLAN ID-based MAC authentication on a switch, use the **mab request format attribute 32 vlan access-vlan** global configuration command. To return to the default setting, use the **no** form of this command.

mab request format attribute 32 vlan access-vlan

no mab request format attribute 32 vlan access-vlan

Syntax Description

This command has no arguments or keywords.

Command Default

VLAN-ID based MAC authentication is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Use this command to allow a RADIUS server to authenticate a new user based on the host MAC address and VLAN.

Use this feature on networks with the Microsoft IAS RADIUS server. The Cisco ACS ignores this command.

Examples

This example shows how to enable VLAN-ID based MAC authentication on a switch:

```
Controller(config)# mab request format attribute 32 vlan access-vlan
```

Related Commands

Command	Description
authentication event	Sets the action for specific authentication events.
authentication fallback	Configures a port to use web authentication as a fallback method for clients that do not support IEEE 802.1x authentication.
authentication host-mode	Sets the authorization manager mode on a port.
authentication open	Enables or disables open access on a port.
authentication order	Sets the order of authentication methods used on a port.
authentication periodic	Enables or disables reauthentication on a port.

Command	Description
authentication port-control	Enables manual control of the port authorization state.
authentication priority	Adds an authentication method to the port-priority list.
authentication timer	Configures the timeout and reauthentication parameters for an 802.1x-enabled port.
authentication violation	Configures the violation modes that occur when a new device connects to a port or when a new device connects to a port with the maximum number of devices already connected to that port.
mab	Enables MAC-based authentication on a port.
mab eap	Configures a port to use the Extensible Authentication Protocol (EAP).
show authentication	Displays information about authentication manager events on the switch.

match (access-map configuration)

To set the VLAN map to match packets against one or more access lists, use the **match** command in access-map configuration mode on the switch stack or on a standalone switch. To remove the match parameters, use the **no** form of this command.

match {**ip address** {*name*| *number*} [*name*| *number*] [*name*| *number*]...| **mac address** {*name*} [*name*] [*name*]...}

no match {**ip address** {*name*| *number*} [*name*| *number*] [*name*| *number*]...| **mac address** {*name*} [*name*] [*name*]...}

Syntax Description

ip address	Sets the access map to match packets against an IP address access list.
mac address	Sets the access map to match packets against a MAC address access list.
name	Name of the access list to match packets against.
number	Number of the access list to match packets against. This option is not valid for MAC access lists.

Command Default

The default action is to have no match parameters applied to a VLAN map.

Command Modes

Access-map configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You enter access-map configuration mode by using the **vlan access-map** global configuration command.

You must enter one access list name or number; others are optional. You can match packets against one or more access lists. Matching any of the lists counts as a match of the entry.

In access-map configuration mode, use the **match** command to define the match conditions for a VLAN map applied to a VLAN. Use the **action** command to set the action that occurs when the packet matches the conditions.

Packets are matched only against access lists of the same protocol type; IP packets are matched against IP access lists, and all other packets are matched against MAC access lists.

Both IP and MAC addresses can be specified for the same map entry.

Examples

This example shows how to define and apply a VLAN access map vmap4 to VLANs 5 and 6 that will cause the interface to drop an IP packet if the packet matches the conditions defined in access list al2:

```
Controller(config)# vlan access-map vmap4
Controller(config-access-map)# match ip address al2
Controller(config-access-map)# action drop
Controller(config-access-map)# exit
Controller(config)# vlan filter vmap4 vlan-list 5-6
```

You can verify your settings by entering the **show vlan access-map** privileged EXEC command.

Related Commands

Command	Description
action	Sets the action for the VLAN access map entry.
show vlan access-map	Displays the VLAN access maps created on the switch.
vlan access-map	Defines a VLAN map and enters access-map configuration mode where you can specify a MAC ACL to match and the action to be taken.

no authentication logging verbose

To filter detailed information from authentication system messages, use the **no authentication logging verbose** global configuration command on the switch stack or on a standalone switch.

no authentication logging verbose

Syntax Description

This command has no arguments or keywords.

Command Default

All details are displayed in the system messages.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

This command filters details, such as anticipated success, from authentication system messages. Failure messages are not filtered.

Examples

To filter verbose authentication system messages:

```
Controller(config)# no authentication logging verbose
```

You can verify your settings by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
no authentication logging verbose	Filters details from authentication system messages.
no dot1x logging verbose	Filters details from 802.1x system messages.
no mab logging verbose	Filters details from MAC authentication bypass (MAB) system messages.

no dot1x logging verbose

To filter detailed information from 802.1x system messages, use the **no dot1x logging verbose** global configuration command on the switch stack or on a standalone switch.

no dot1x logging verbose

Syntax Description

This command has no arguments or keywords.

Command Default

All details are displayed in the system messages.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

This command filters details, such as anticipated success, from 802.1x system messages. Failure messages are not filtered.

Examples

To filter verbose 802.1x system messages:

```
Controller(config)# no dot1x logging verbose
```

You can verify your settings by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
no authentication logging verbose	Filters details from authentication system messages.
no dot1x logging verbose	Filters details from 802.1x system messages.
no mab logging verbose	Filters details from MAC authentication bypass (MAB) system messages.

no mab logging verbose

To filter detailed information from MAC authentication bypass (MAB) system messages, use the **no mab logging verbose** global configuration command on the switch stack or on a standalone switch.

no mab logging verbose

Syntax Description

This command has no arguments or keywords.

Command Default

All details are displayed in the system messages.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

This command filters details, such as anticipated success, from MAC authentication bypass (MAB) system messages. Failure messages are not filtered.

Examples

To filter verbose MAB system messages:

```
Controller(config)# no mab logging verbose
```

You can verify your settings by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
no authentication logging verbose	Filters details from authentication system messages.
no dot1x logging verbose	Filters details from 802.1x system messages.
no mab logging verbose	Filters details from MAC authentication bypass (MAB) system messages.

permit (MAC access-list configuration)

To allow non-IP traffic to be forwarded if the conditions are matched, use the **permit** MAC access-list configuration command on the switch stack or on a standalone switch. To remove a permit condition from the extended MAC access list, use the **no** form of this command.

{**permit** {**any** | **host***src-MAC-addr* | *src-MAC-addr mask*} {**any** | **host***dst-MAC-addr* | *dst-MAC-addr mask*} [*type mask* | **aarp** | **amber** | **appletalk** | **dec-spanning** | **decnet-iv** | **diagnostic** | **dsm** | **etype-6000** | **etype-8042** | **lat** | **lavc-sca** | **lsap***lsap mask* | **mop-console** | **mop-dump** | **msdos** | **mumps** | **netbios** | **vines-echo** | **vines-ip** | **xns-idp**][**cos***cos*]

nopermit {**any** | **host** *src-MAC-addr* | *src-MAC-addr mask*} {**any** | **host** *dst-MAC-addr* | *dst-MAC-addr mask*} [*type mask* | **aarp** | **amber** | **appletalk** | **dec-spanning** | **decnet-iv** | **diagnostic** | **dsm** | **etype-6000** | **etype-8042** | **lat** | **lavc-sca** | **lsap** *lsap mask* | **mop-console** | **mop-dump** | **msdos** | **mumps** | **netbios** | **vines-echo** | **vines-ip** | **xns-idp**][**cos***cos*]

Syntax Description

any	Denies any source or destination MAC address.
host *src-MAC-addr* | *src-MAC-addr mask*	Specifies a host MAC address and optional subnet mask. If the source address for a packet matches the defined address, non-IP traffic from that address is denied.
host *dst-MAC-addr* | *dst-MAC-addr mask*	Specifies a destination MAC address and optional subnet mask. If the destination address for a packet matches the defined address, non-IP traffic to that address is denied.
type mask	(Optional) Specifies the Ethertype number of a packet with Ethernet II or SNAP encapsulation to identify the protocol of the packet. • *type* is 0 to 65535, specified in hexadecimal. • *mask* is a mask of don't care bits applied to the Ethertype before testing for a match.
aarp	(Optional) Specifies Ethertype AppleTalk Address Resolution Protocol that maps a data-link address to a network address.
amber	(Optional) Specifies EtherType DEC-Amber.
appletalk	(Optional) Specifies EtherType AppleTalk/EtherTalk.
dec-spanning	(Optional) Specifies EtherType Digital Equipment Corporation (DEC) spanning tree.
decnet-iv	(Optional) Specifies EtherType DECnet Phase IV protocol.
diagnostic	(Optional) Specifies EtherType DEC-Diagnostic.
dsm	(Optional) Specifies EtherType DEC-DSM.

etype-6000	(Optional) Specifies EtherType 0x6000.
etype-8042	(Optional) Specifies EtherType 0x8042.
lat	(Optional) Specifies EtherType DEC-LAT.
lavc-sca	(Optional) Specifies EtherType DEC-LAVC-SCA.
lsap *lsap-number mask*	(Optional) Specifies the LSAP number (0 to 65535) of a packet with 802.2 encapsulation to identify the protocol of the packet. The *mask* is a mask of don't care bits applied to the LSAP number before testing for a match.
mop-console	(Optional) Specifies EtherType DEC-MOP Remote Console.
mop-dump	(Optional) Specifies EtherType DEC-MOP Dump.
msdos	(Optional) Specifies EtherType DEC-MSDOS.
mumps	(Optional) Specifies EtherType DEC-MUMPS.
netbios	(Optional) Specifies EtherType DEC- Network Basic Input/Output System (NETBIOS).
vines-echo	(Optional) Specifies EtherType Virtual Integrated Network Service (VINES) Echo from Banyan Systems.
vines-ip	(Optional) Specifies EtherType VINES IP.
xns-idp	(Optional) Specifies EtherType Xerox Network Systems (XNS) protocol suite.
cos *cos*	(Optional) Specifies an arbitrary class of service (CoS) number from 0 to 7 to set priority. Filtering on CoS can be performed only in hardware. A warning message appears if the **cos** option is configured.

Command Default

This command has no defaults. However, the default action for a MAC-named ACL is to deny.

Command Modes

MAC access-list configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Though visible in the command-line help strings, **appletalk** is not supported as a matching condition.

You enter MAC access-list configuration mode by using the **mac access-list extended** global configuration command.

If you use the **host** keyword, you cannot enter an address mask; if you do not use the **any** or **host** keywords, you must enter an address mask.

After an access control entry (ACE) is added to an access control list, an implied **deny-any-any** condition exists at the end of the list. That is, if there are no matches, the packets are denied. However, before the first ACE is added, the list permits all packets.

To filter IPX traffic, you use the *type mask* or **lsap** *lsap mask* keywords, depending on the type of IPX encapsulation being used. Filter criteria for IPX encapsulation types as specified in Novell terminology and Cisco IOS terminology are listed in the following table.

Table 12: IPX Filtering Criteria

IPX Encapsulation Type		Filter Criterion
Cisco IOS Name	**Novell Name**	
arpa	Ethernet II	Ethertype 0x8137
snap	Ethernet-snap	Ethertype 0x8137
sap	Ethernet 802.2	LSAP 0xE0E0
novell-ether	Ethernet 802.3	LSAP 0xFFFF

Examples

This example shows how to define the MAC-named extended access list to allow NETBIOS traffic from any source to MAC address 00c0.00a0.03fa. Traffic matching this list is allowed.

```
Controller(config-ext-macl)# permit any host 00c0.00a0.03fa netbios
```

This example shows how to remove the permit condition from the MAC-named extended access list:

```
Controller(config-ext-macl)# no permit any 00c0.00a0.03fa 0000.0000.0000 netbios
```

This example permits all packets with Ethertype 0x4321:

```
Controller(config-ext-macl)# permit any any 0x4321 0
```

You can verify your settings by entering the **show access-lists** privileged EXEC command.

Related Commands

Command	Description
deny	Denies from the MAC access-list configuration. Denies non-IP traffic to be forwarded if conditions are matched.

Command	Description
mac access-list extended	Creates an access list based on MAC addresses for non-IP traffic.
show access-lists	Displays access control lists configured on a switch.

protocol (IPv6 snooping)

To specify that addresses should be gleaned with Dynamic Host Configuration Protocol (DHCP) or Neighbor Discovery Protocol (NDP), or to associate the protocol with an IPv6 prefix list, use the **protocol** command. To disable address gleaning with DHCP or NDP, use the **no** form of the command.

protocol { **dhcp** | **ndp** }

protocol { **dhcp** | **ndp** }

Syntax Description

dhcp	Specifies that addresses should be gleaned in Dynamic Host Configuration Protocol (DHCP) packets.
ndp	Specifies that addresses should be gleaned in Neighbor Discovery Protocol (NDP) packets.

Command Default

Snooping and recovery are attempted using both DHCP and NDP.

Command Modes

IPv6 snooping configuration mode (config-ipv6-snooping)

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

If an address does not match the prefix list associated with DHCP or NDP, then control packets will be dropped and recovery of the binding table entry will not be attempted with that protocol.

- Using the **no protocol** {**dhcp** | **ndp**} command indicates that a protocol will not be used for snooping or gleaning.
- If the **no protocol dhcp** command is used, DHCP can still be used for binding table recovery.
- Data glean can recover with DHCP and NDP, though destination guard will only recovery through DHCP.

Examples

This example shows how to define an IPv6 snooping policy name as policy1, place the switch in IPv6 snooping policy configuration mode, and configure the port to use DHCP to glean addresses:

```
Controller(config)# ipv6 snooping policy policy1
Controller(config-ipv6-snooping)# protocol dhcp
```

security level (IPv6 snooping)

To specify the level of security enforced, use the **security-level** command in IPv6 snooping policy configuration mode.

security level {**glean** | **guard** | **inspect**}

Syntax Description

glean	Extracts addresses from the messages and installs them into the binding table without performing any verification.
guard	Performs both glean and inspect. Additionally, RA and DHCP server messages are rejected unless they are received on a trusted port or another policy authorizes them.
inspect	Validates messages for consistency and conformance; in particular, address ownership is enforced. Invalid messages are dropped.

Command Default

The default security level is guard.

Command Modes

IPv6 snooping configuration (config-ipv6-snooping)

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Examples

This example shows how to define an IPv6 snooping policy name as policy1, place the device in IPv6 snooping configuration mode, and configure the security level as inspect:

```
Controller(config)# ipv6 snooping policy policy1
Controller(config-ipv6-snooping)# security-level inspect
```

security passthru

To modify the IPsec pass-through, use the **security passthru** command. To disable, use the no form of the command.

security passthru *ip-address*

no security passthru

Syntax Description

ip-address	IP address of the IPsec gateway (router) that is terminating the VPN tunnel.

Command Default

None.

Command Modes

wlan

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

None.

Examples

This example shows how to modify IPSec pass-through.

```
Controller#configre terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)#security passthrough 10.1.1.1
```

show aaa clients

To show AAA client statistics, use the **show aaa clients** command.

show aaa clients [**detailed**]

Syntax Description

detailed	(Optional) Shows detailed AAA client statistics.

Command Modes

User EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This is an example of output from the **show aaa clients** command:

```
Controller# show aaa clients
Dropped request packets: 0
```

show aaa command handler

To show AAA command handler statistics, use the **show aaa command handler** command.

show aaa command handler

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This is an example of output from the **show aaa command handler** command:

```
Controller# show aaa command handler

AAA Command Handler Statistics:
    account-logon: 0, account-logoff: 0
    account-query: 0, pod: 0
    service-logon: 0, service-logoff: 0
    user-profile-push: 0, session-state-log: 0
    reauthenticate: 0, bounce-host-port: 0
    disable-host-port: 0, update-rbacl: 0
    update-sgt: 0, update-cts-policies: 0
    invalid commands: 0
    async message not sent: 0
```

show aaa local

To show AAA local method options, use the **show aaa local** command.

show aaa local {**netuser** {*name* | **all** } | **statistics** | **user lockout**}

Syntax Description

netuser	Specifies the AAA local network or guest user database.
name	Network user name.
all	Specifies the network and guest user information.
statistics	Displays statistics for local authentication.
user lockout	Specifies the AAA local locked-out user.

Command Modes

User EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This is an example of output from the **show aaa local statistics** command:

```
Controller# show aaa local statistics

Local EAP statistics

EAP Method         Success       Fail
---------------------------------------
Unknown                  0          0
EAP-MD5                  0          0
EAP-GTC                  0          0
LEAP                     0          0
PEAP                     0          0
EAP-TLS                  0          0
EAP-MSCHAPV2             0          0
EAP-FAST                 0          0

Requests received from AAA:                  0
Responses returned from EAP:                 0
Requests dropped (no EAP AVP):               0
Requests dropped (other reasons):            0
Authentication timeouts from EAP:            0

Credential request statistics
Requests sent to backend:                    0
Requests failed (unable to send):            0
Authorization results received

  Success:                                   0
```

```
Fail:                                    0
```

show aaa servers

To shows all AAA servers as seen by the AAA server MIB, use the **show aaa servers** command.

show aaa servers [**private**|**public**|[**detailed**]]

Syntax Description

detailed	(Optional) Displays private AAA servers as seen by the AAA Server MIB.
public	(Optional) Displays public AAA servers as seen by the AAA Server MIB.
detailed	(Optional) Displays detailed AAA server statistics.

Command Modes

User EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This is an example of output from the **show aaa servers** command:

```
Controller# show aaa servers
RADIUS: id 1, priority 1, host 172.20.128.2, auth-port 1645, acct-port 1646
State: current UP, duration 9s, previous duration 0s
Dead: total time 0s, count 0
Quarantined: No
Authen: request 0, timeouts 0, failover 0, retransmission 0
Response: accept 0, reject 0, challenge 0
Response: unexpected 0, server error 0, incorrect 0, time 0ms
Transaction: success 0, failure 0
Throttled: transaction 0, timeout 0, failure 0
Author: request 0, timeouts 0, failover 0, retransmission 0
Response: accept 0, reject 0, challenge 0
Response: unexpected 0, server error 0, incorrect 0, time 0ms
Transaction: success 0, failure 0
Throttled: transaction 0, timeout 0, failure 0
Account: request 0, timeouts 0, failover 0, retransmission 0
Request: start 0, interim 0, stop 0
Response: start 0, interim 0, stop 0
Response: unexpected 0, server error 0, incorrect 0, time 0ms
Transaction: success 0, failure 0
Throttled: transaction 0, timeout 0, failure 0
Elapsed time since counters last cleared: 0m
Estimated Outstanding Access Transactions: 0
Estimated Outstanding Accounting Transactions: 0
Estimated Throttled Access Transactions: 0
Estimated Throttled Accounting Transactions: 0
Maximum Throttled Transactions: access 0, accounting 0
```

show aaa sessions

To show AAA sessions as seen by the AAA Session MIB, use the **show aaa sessions** command.

show aaa sessions

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This is an example of output from the **show aaa sessions** command:

```
Controller# show aaa sessions
Total sessions since last reload: 7
Session Id: 4007
   Unique Id: 4025
   User Name: *not available*
   IP Address: 0.0.0.0
   Idle Time: 0
   CT Call Handle: 0
```

show authentication history

To display the authenticated sessions alive on the device, use the **show authentication history** command.

show authentication history [**min-uptime** *seconds*]

Syntax Description

min-uptime *seconds*	(Optional) Displays sessions within the minimum uptime. The range is from 1 through 4294967295 seconds.

Command Modes

User EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Use the **show authentication history** command to display the authenticated sessions alive on the device.

Examples

This is an example of output from the **show authentication history** command:

```
Controller# show authentication history
Interface  MAC Address     Method  Domain  Status  Uptime
Gi3/0/2    0021.d864.07c0  dot1x   DATA    Auth    38s

Session count = 1
```

show authentication sessions

To display information about current Auth Manager sessions, use the **show authentication sessions** command.

show authentication sessions [**database**][**handle** *handle-id* [**details**]][**interface** *type number* [**details**][**mac** *mac-address* [**interface** *type number*][**method** *method-name* [**interface** *type number* [**details**] [**session-id** *session-id* [**details**]]

Syntax Description

database	(Optional) Shows only data stored in session database.
handle *handle-id*	(Optional) Specifies the particular handle for which Auth Manager information is to be displayed.
details	(Optional) Shows detailed information.
interface *type number*	(Optional) Specifies a particular interface type and number for which Auth Manager information is to be displayed.
mac *mac-address*	(Optional) Specifies the particular MAC address for which you want to display information.
method *method-name*	(Optional) Specifies the particular authentication method for which Auth Manager information is to be displayed. If you specify a method (**dot1x**, **mab**, or **webauth**), you may also specify an interface.
session-id *session-id*	(Optional) Specifies the particular session for which Auth Manager information is to be displayed.

Command Modes

User EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Use the **show authentication sessions** command to display information about all current Auth Manager sessions. To display information about specific Auth Manager sessions, use one or more of the keywords.

This table shows the possible operating states for the reported authentication sessions.

Table 13: Authentication Method States

State	Description
Not run	The method has not run for this session.
Running	The method is running for this session.
Failed over	The method has failed and the next method is expected to provide a result.
Success	The method has provided a successful authentication result for the session.
Authc Failed	The method has provided a failed authentication result for the session.

This table shows the possible authentication methods.

Table 14: Authentication Method States

State	Description
dot1x	802.1X
mab	MAC authentication bypass
webauth	web authentication

Examples

The following example shows how to display all authentication sessions on the switch:

```
Controller# show authentication sessions
Interface    MAC Address     Method   Domain   Status         Session ID
Gi1/0/48     0015.63b0.f676  dot1x    DATA     Authz Success  0A3462B1000000102983C05C
Gi1/0/5      000f.23c4.a401  mab      DATA     Authz Success  0A3462B10000000D24F80B58
Gi1/0/5      0014.bf5d.d26d  dot1x    DATA     Authz Success  0A3462B10000000E29811B94
```

The following example shows how to display all authentication sessions on an interface:

```
Controller# show authentication sessions interface gigabitethernet2/0/47
            Interface:  GigabitEthernet2/0/47
          MAC Address:  Unknown
           IP Address:  Unknown
               Status:  Authz Success
               Domain:  DATA
       Oper host mode:  multi-host
     Oper control dir:  both
        Authorized By:  Guest Vlan
          Vlan Policy:  20
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0A3462C8000000000002763C
      Acct Session ID:  0x00000002
```

```
               Handle:  0x25000000
Runnable methods list:
       Method   State
       mab      Failed over
       dot1x    Failed over
----------------------------------------
            Interface:  GigabitEthernet2/0/47
          MAC Address:  0005.5e7c.da05
           IP Address:  Unknown
            User-Name:  00055e7cda05
               Status:  Authz Success
               Domain:  VOICE
      Oper host mode:  multi-domain
     Oper control dir:  both
        Authorized By:  Authentication Server
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0A3462C8000000010002A238
      Acct Session ID:  0x00000003
               Handle:  0x91000001
Runnable methods list:
       Method   State
       mab      Authc Success
       dot1x    Not run
```

show cisp

To display CISP information for a specified interface, use the **show cisp** privileged EXEC command.

show cisp {[**clients** | **interface** *interface-id*] | **registrations** | **summary**}

Syntax Description

clients	(Optional) Display CISP client details.
interface *interface-id*	(Optional) Display CISP information about the specified interface. Valid interfaces include physical ports and port channels.
registrations	Displays CISP registrations.
summary	(Optional) Displays CISP summary.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows output from the **show cisp interface** command:

```
Controller# show cisp interface fast 0
CISP not enabled on specified interface
```

This example shows output from the **show cisp registration** command:

```
Controller# show cisp registrations
Interface(s) with CISP registered user(s):
-----------------------------------------
Fa1/0/13
Auth Mgr (Authenticator)
Gi2/0/1
Auth Mgr (Authenticator)
Gi2/0/2
Auth Mgr (Authenticator)
Gi2/0/3
Auth Mgr (Authenticator)
Gi2/0/5
Auth Mgr (Authenticator)
Gi2/0/9
Auth Mgr (Authenticator)
Gi2/0/11
Auth Mgr (Authenticator)
Gi2/0/13
Auth Mgr (Authenticator)
Gi3/0/3
Gi3/0/5
```

```
Gi3/0/23
```

Related Commands

Command	Description
cisp enable	Enable Client Information Signalling Protocol (CISP)
dot1x credentials *profile*	Configure a profile on a supplicant switch

show dot1x

To display IEEE 802.1x statistics, administrative status, and operational status for the switch or for the specified port, use the **show dot1x** user EXEC command.

show dot1x [**all** [**count** | **details** | **statistics** | **summary**]] [**interface** *type number* [**details** | **statistics**]] [**statistics**]

Syntax Description

all	(Optional) Displays the IEEE 802.1x information for all interfaces.
count	(Optional) Displays total number of authorized and unauthorized clients.
details	(Optional) Displays the IEEE 802.1x interface details.
statistics	(Optional) Displays the IEEE 802.1x statistics for all interfaces.
summary	(Optional) Displays the IEEE 802.1x summary for all interfaces.
interface *type number*	(Optional) Displays the IEEE 802.1x status for the specified port.

Command Modes

User EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This is an example of output from the **show dot1x all** command:

```
Controller# show dot1x all
Sysauthcontrol              Enabled
Dot1x Protocol Version            3
```

This is an example of output from the **show dot1x all count** command:

```
Controller# show dot1x all count
Number of Dot1x sessions
------------------------------
Authorized Clients        = 0
UnAuthorized Clients      = 0
Total No of Client        = 0
```

This is an example of output from the **show dot1x all statistics** command:

```
Controller# show dot1x statistics
Dot1x Global Statistics for
```

```
-----------------------------------------------
RxStart = 0     RxLogoff = 0    RxResp = 0      RxRespID = 0
RxReq = 0       RxInvalid = 0   RxLenErr = 0
RxTotal = 0

TxStart = 0     TxLogoff = 0    TxResp = 0
TxReq = 0       ReTxReq = 0     ReTxReqFail = 0
TxReqID = 0     ReTxReqID = 0   ReTxReqIDFail = 0
TxTotal = 0
```

show eap pac peer

To display stored Protected Access Credentials (PAC) for Extensible Authentication Protocol (EAP) Flexible Authentication via Secure Tunneling (FAST) peers, use the **show eap pac peer** privileged EXEC command.

show eap pac peer

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This is an example of output from the **show eap pac peers** privileged EXEC command:

```
Controller> show eap pac peers
No PACs stored
```

Related Commands

Command	Description
clear eap sessions	Clears EAP session information for the switch or for the specified port.

show ip dhcp snooping statistics

Use the **show ip dhcp snooping statistics** user EXEC command to display DHCP snooping statistics in summary or detail form.

show ip dhcp snooping statistics [**detail**]

Syntax Description

detail	(Optional) Displays detailed statistics information.

Command Modes

User EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

In a switch stack, all statistics are generated on the stack master. If a new active switch is elected, the statistics counters reset.

Examples

This is an example of output from the **show ip dhcp snooping statistics** command:

```
Controller> show ip dhcp snooping statistics

 Packets Forwarded                                    = 0
 Packets Dropped                                      = 0
 Packets Dropped From untrusted ports                 = 0
```

This is an example of output from the **show ip dhcp snooping statistics detail** command:

```
Controller> show ip dhcp snooping statistics detail

 Packets Processed by DHCP Snooping                   = 0
 Packets Dropped Because
   IDB not known                                      = 0
   Queue full                                         = 0
   Interface is in errdisabled                        = 0
   Rate limit exceeded                                = 0
   Received on untrusted ports                        = 0
   Nonzero giaddr                                     = 0
   Source mac not equal to chaddr                     = 0
   Binding mismatch                                   = 0
   Insertion of opt82 fail                            = 0
   Interface Down                                     = 0
   Unknown output interface                           = 0
   Reply output port equal to input port              = 0
   Packet denied by platform                          = 0
```

This table shows the DHCP snooping statistics and their descriptions:

Table 15: DHCP Snooping Statistics

DHCP Snooping Statistic	Description
Packets Processed by DHCP Snooping	Total number of packets handled by DHCP snooping, including forwarded and dropped packets.
Packets Dropped Because IDB not known	Number of errors when the input interface of the packet cannot be determined.
Queue full	Number of errors when an internal queue used to process the packets is full. This might happen if DHCP packets are received at an excessively high rate and rate limiting is not enabled on the ingress ports.
Interface is in errdisabled	Number of times a packet was received on a port that has been marked as error disabled. This might happen if packets are in the processing queue when a port is put into the error-disabled state and those packets are subsequently processed.
Rate limit exceeded	Number of times the rate limit configured on the port was exceeded and the interface was put into the error-disabled state.
Received on untrusted ports	Number of times a DHCP server packet (OFFER, ACK, NAK, or LEASEQUERY) was received on an untrusted port and was dropped.
Nonzero giaddr	Number of times the relay agent address field (giaddr) in the DHCP packet received on an untrusted port was not zero, or the **no ip dhcp snooping information option allow-untrusted** global configuration command is not configured and a packet received on an untrusted port contained option-82 data.
Source mac not equal to chaddr	Number of times the client MAC address field of the DHCP packet (chaddr) does not match the packet source MAC address and the **ip dhcp snooping verify mac-address** global configuration command is configured.
Binding mismatch	Number of times a RELEASE or DECLINE packet was received on a port that is different than the port in the binding for that MAC address-VLAN pair. This indicates someone might be trying to spoof the real client, or it could mean that the client has moved to another port on the switch and issued a RELEASE or DECLINE. The MAC address is taken from the chaddr field of the DHCP packet, not the source MAC address in the Ethernet header.
Insertion of opt82 fail	Number of times the option-82 insertion into a packet failed. The insertion might fail if the packet with the option-82 data exceeds the size of a single physical packet on the internet.

DHCP Snooping Statistic	Description
Interface Down	Number of times the packet is a reply to the DHCP relay agent, but the SVI interface for the relay agent is down. This is an unlikely error that occurs if the SVI goes down between sending the client request to the DHCP server and receiving the response.
Unknown output interface	Number of times the output interface for a DHCP reply packet cannot be determined by either option-82 data or a lookup in the MAC address table. The packet is dropped. This can happen if option 82 is not used and the client MAC address has aged out. If IPSG is enabled with the port-security option and option 82 is not enabled, the MAC address of the client is not learned, and the reply packets will be dropped.
Reply output port equal to input port	Number of times the output port for a DHCP reply packet is the same as the input port, causing a possible loop. Indicates a possible network misconfiguration or misuse of trust settings on ports.
Packet denied by platform	Number of times the packet has been denied by a platform-specific registry.

show radius server-group

To display properties for the RADIUS server group, use the **show radius server-group** command.

show radius server-group {*name* | **all**}

Syntax Description

name	Name of the server group. The character string used to name the group of servers must be defined using **the aaa group server radius** command.
all	Displays properties for all of the server groups.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Use the **show radius server-group** command to display the server groups that you defined by using the **aaa group server radius** command.

Examples

This is an example of output from the **show radius server-group all** command:

```
Controller# show radius server-group all
Server group radius
    Sharecount = 1  sg_unconfigured = FALSE
    Type = standard  Memlocks = 1
```

This table describes the significant fields shown in the display.

Table 16: show radius server-group command Field Descriptions

Field	Description
Server group	Name of the server group.
Sharecount	Number of method lists that are sharing this server group. For example, if one method list uses a particular server group, the sharecount would be 1. If two method lists use the same server group, the sharecount would be 2.

Field	Description
sg_unconfigured	Server group has been unconfigured.
Type	The type can be either standard or nonstandard. The type indicates whether the servers in the group accept nonstandard attributes. If all servers within the group are configured with the nonstandard option, the type will be shown as "nonstandard".
Memlocks	An internal reference count for the server-group structure that is in memory. The number represents how many internal data structure packets or transactions are holding references to this server group. Memlocks is used internally for memory management purposes.

show vlan access-map

To display information about a particular VLAN access map or for all VLAN access maps, use the **show vlan access-map** command in privileged EXEC mode

show vlan access-map [*map-name*]

Syntax Description

map-name	(Optional) Name of a specific VLAN access map.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This is an example of output from the **show vlan access-map** command:

Related Commands

Command	Description
show vlan filter	Displays information about all VLAN filters or about a particular VLAN or VLAN access map.
vlan access-map	Defines a VLAN map and enters access-map configuration mode where you can specify a MAC ACL to match and the action to be taken.
vlan filter	Applies a VLAN map to one or more VLANs.

show vlan filter

To display information about all VLAN filters or about a particular VLAN or VLAN access map, use the **show vlan filter** command in privileged EXEC mode.

show vlan filter {**access-map** *name*| **vlan** *vlan-id*}

Syntax Description

access-map *name*	(Optional) Displays filtering information for the specified VLAN access map.
vlan *vlan-id*	(Optional) Displays filtering information for the specified VLAN. The range is 1 to 4094.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This is an example of output from the **show vlan filter** command:

```
Controller# show vlan filter
VLAN Map map_1 is filtering VLANs:
  20-22
```

Related Commands

Command	Description
show vlan access-map	Displays the VLAN access maps created on the switch.
vlan access-map	Defines a VLAN map and enters access-map configuration mode where you can specify a MAC ACL to match and the action to be taken.
vlan filter	Applies a VLAN map to one or more VLANs.

show vlan group

To display the VLANs that are mapped to VLAN groups, use the **show vlan group** command in privileged EXEC mode.

show vlan group [**group-name** *vlan-group-name* **[user_count]**]

Syntax Description

group-name *vlan-group-name*	(Optional) Displays the VLANs mapped to the specified VLAN group.
user_count	(Optional) Displays the number of users in each VLAN mapped to a specified VLAN group.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The **show vlan group** command displays the existing VLAN groups and lists the VLANs and VLAN ranges that are members of each VLAN group. If you enter the **group-name** keyword, only the members of the specified VLAN group are displayed.

Examples

This example shows how to display the members of a specified VLAN group:

This example shows how to display number of users in each of the VLANs in a group:

```
Controller# show vlan group group-name group2 user_count
  VLAN     : Count
--------------------
  40         : 5
  41         : 8
  42         : 12
  43         : 2
  44         : 9
  45         : 0
```

Related Commands

Command	Description
vlan group	Creates or modifies a VLAN group.

tracking (IPv6 snooping)

To override the default tracking policy on a port, use the **tracking** command in IPv6 snooping policy configuration mode.

tracking {**enable** [**reachable-lifetime** {*value* | **infinite**}] | **disable** [**stale-lifetime** {*value* | **infinite**}

Syntax Description

enable	Enables tracking.
reachable-lifetime	(Optional) Specifies the maximum amount of time a reachable entry is considered to be directly or indirectly reachable without proof of reachability. • The **reachable-lifetime** keyword can be used only with the **enable** keyword. • Use of the **reachable-lifetime** keyword overrides the global reachable lifetime configured by the **ipv6 neighbor binding reachable-lifetime** command.
value	Lifetime value, in seconds. The range is from 1 to 86400, and the default is 300.
infinite	Keeps an entry in a reachable or stale state for an infinite amount of time.
disable	Disables tracking.
stale-lifetime	(Optional) Keeps the time entry in a stale state, which overwrites the global stale-lifetime configuration. • The stale lifetime is 86,400 seconds. • The **stale-lifetime** keyword can be used only with the **disable** keyword. • Use of the **stale-lifetime** keyword overrides the global stale lifetime configured by the **ipv6 neighbor binding stale-lifetime** command.

Command Default

The time entry is kept in a reachable state.

Command Modes

IPv6 snooping configuration (config-ipv6-snooping)

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The **tracking** command overrides the default tracking policy set by the **ipv6 neighbor tracking** command on the port on which this policy applies. This function is useful on trusted ports where, for example, you may not want to track entries but want an entry to stay in the binding table to prevent it from being stolen.

The **reachable-lifetime** keyword is the maximum time an entry will be considered reachable without proof of reachability, either directly through tracking or indirectly through IPv6 snooping. After the **reachable-lifetime** value is reached, the entry is moved to stale. Use of the **reachable-lifetime** keyword with the tracking command overrides the global reachable lifetime configured by the **ipv6 neighbor binding reachable-lifetime** command.

The **stale-lifetime** keyword is the maximum time an entry is kept in the table before it is deleted or the entry is proven to be reachable, either directly or indirectly. Use of the **reachable-lifetime** keyword with the **tracking** command overrides the global stale lifetime configured by the **ipv6 neighbor binding stale-lifetime** command.

Examples

This example shows how to define an IPv6 snooping policy name as policy1, place the switch in IPv6 snooping policy configuration mode, and configure an entry to stay in the binding table for an infinite length of time on a trusted port:

```
Controller(config)# ipv6 snooping policy policy1
Controller(config-ipv6-snooping)# tracking disable stale-lifetime infinite
```

trusted-port

To configure a port to become a trusted port, use the **trusted-port** command in IPv6 snooping policy mode or ND inspection policy configuration mode. To disable this function, use the **no** form of this command.

trusted-port

no trusted-port

Syntax Description

This command has no arguments or keywords.

Command Default

No ports are trusted.

Command Modes

ND inspection policy configuration (config-nd-inspection)

IPv6 snooping configuration (config-ipv6-snooping)

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

When the **trusted-port** command is enabled, limited or no verification is performed when messages are received on ports that have this policy. However, to protect against address spoofing, messages are analyzed so that the binding information that they carry can be used to maintain the binding table. Bindings discovered from these ports will be considered more trustworthy than bindings received from ports that are not configured to be trusted.

Examples

This example shows how to define an NDP policy name as policy1, place the switch in NDP inspection policy configuration mode, and configure the port to be trusted:

```
Controller(config)# ipv6  nd inspection  policy1
Controller(config-nd-inspection)# trusted-port
```

This example shows how to define an IPv6 snooping policy name as policy1, place the switch in IPv6 snooping policy configuration mode, and configure the port to be trusted:

```
Controller(config)# ipv6 snooping policy policy1
Controller(config-ipv6-snooping)# trusted-port
```

wireless dot11-padding

To enable over-the-air frame padding, use the **wireless dot11-padding** command. To disable, use the no form of the command.

wireless dot11-padding

no wireless dot11-padding

Command Default

Disabled.

Command Modes

config

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

None.

Examples

This example shows how to enable over-the-air frame padding

```
Controller#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)#wireless dot11-padding
```

wireless security dot1x

To configure IEEE 802.1x global configurations, use the **wireless security dot1x** command.

wireless security dot1x [**eapol-key** {**retries** *retries*| **timeout** *milliseconds*}| **group-key interval** *sec*| **identity-request** {**retries** *retries*| **timeout** *seconds*}| **radius [call-station-id]** {**ap-macaddress**| **ap-macaddress-ssid**| **ipaddress**| **macaddress**}| **request** {**retries** *retries*| **timeout** *seconds*}| **wep key** {**index 0**| **index 3**}]

Syntax Description

eapol-key	Configures eapol-key related parameters.
retries *retries*	(Optional) Specifies the maximum number of times (0 to 4 retries) that the controller retransmits an EAPOL (WPA) key message to a wireless client. The default value is 2.
timeout *milliseconds*	(Optional) Specifies the amount of time (200 to 5000 milliseconds) that the controller waits before retransmitting an EAPOL (WPA) key message to a wireless client using EAP or WPA/WPA-2 PSK. The default value is 1000 milliseconds.
group-key interval *sec*	Configures EAP-broadcast key renew interval time in seconds (120 to 86400 seconds).
identity-request	Configures EAP ID request related parameters.
retries *retries*	(Optional) Specifies the maximum number of times (0 to 4 retries) that the controller request the EAP ID. The default value is 2.
timeout *seconds*	(Optional) Specifies the amount of time (1 to 120 seconds) that the controller waits before retransmitting an EAP Identity Request message to a wireless client. The default value is 30 seconds.
radius	Configures radius messages.
call-station-id	(Optional) Configures Call-Station Id sent in radius messages.
ap-macaddress	Sets Call Station Id Type to the AP's MAC Address.
ap-macaddress-ssid	Sets Call Station Id Type to 'AP MAC address':'SSID'.
ipaddress	Sets Call Station Id Type to the system's IP Address.
macaddress	Sets Call Station Id Type to the system's MAC Address.
request	Configures EAP request related parameters.

retries *retries*	(Optional) For EAP messages other than Identity Requests or EAPOL (WPA) key messages, specifies the maximum number of times (0 to 20 retries) that the controller retransmits the message to a wireless client. The default value is 2.
timeout *seconds*	(Optional) For EAP messages other than Identity Requests or EAPOL (WPA) key messages, specifies the amount of time (1 to 120 seconds) that the controller waits before retransmitting the message to a wireless client. The default value is 30 seconds.
wep key	Configures 802.1x WEP related paramters.
index 0	Specifies the WEP key index value as 0
index 3	Specifies the WEP key index value as 3

Command Default

Default for eapol-key-timeout: 1 second.

Default for eapol-key-retries: 2 retries.

Command Modes

config

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

None.

Examples

This example lists all the commands under **wireless security dot1x** .

```
Controller#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)#wireless security dot1x ?
  eapol-key         Configure eapol-key related parameters
  group-key         Configures EAP-broadcast key renew interval time in seconds
  identity-request  Configure EAP ID request related parameters
  radius            Configure radius messages
  request           Configure EAP request related parameters
  wep               Configure 802.1x WEP related paramters
  <cr>
```

wireless security lsc

To configure locally significant certificates, use the **wireless security lsc** command.

wireless security lsc {**ap-provision** [**auth-list** *mac-addr*| **revert** *number*]| **other-params** *key-size*| **subject-params** *country state city orgn dept email*| **trustpoint** *trustpoint*}

Syntax Description

ap-provision	Specifies the access point provision list settings.
auth-list *mac-addr*	Specifies the provision list authorization settings.
revert *number*	Specifies the number of times the access point attempts to join the controller using an LSC before reverting to the default certificate. The maximum number of attempts cannot exceed 255.
other-params *key-size*	Specifies the device certificate key size settings.
subject-params *country state city orgn dept email*	Specifies the device certificate settings. Country, state, city, organization, department, and email of the certificate authority.
trustpoint *trustpoint*	Specifies the LSC Trustpoint.

Command Default

None

Command Modes

config

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You can configure only one CA server. To configure a different CA server, delete the configured CA server by using the config certificate lsc ca-server delete command, and then configure a different CA server.

If you configure an access point provision list, only the access points in the provision list are provisioned when you enable AP provisioning (in Step 8). If you do not configure an access point provision list, all access points with an MIC or SSC certificate that join the controller are LSC provisioned.

Examples

This example shows how to

```
Controller#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)#wireless security lsc ?
  ap-provision    Provisioning the AP's with LSC's
```

```
other-params    Configure Other Parameters for Device Certs
subject-params  Configure the Subject Parameters for Device Certs
trustpoint      Configure LSC Trustpoint
<cr>
```

wireless security strong-password

To configure strong password enforcement options, use the **wireless security strong-password** command. To disable strong password, use the no form of the command.

wireless security strong-password

no wireless security strong-password

Command Default

None.

Command Modes

config

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

None.

Examples

This example shows how to configure a strong-password for wireless security.

```
Controller#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)#wireless security strong-password
```

wireless wps ap-authentication

To configure the access point neighbor authentication, use the **wireless wps ap-authentication** command. To remove the access point neighbor authentication, use the no form of the command.

wireless wps ap-authentication [**threshold** *value*]

no wireless wps ap-authentication [threshold]

Syntax Description

threshold *value*	Specifies that the WMM-enabled clients are on the wireless LAN. Threshold value (1 to 255).

Command Default

None.

Command Modes

config

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

None.

Examples

This example shows how to set the threshold value for WMM-enabled clients.

```
Controller#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)#wireless wps ap-authentication threshold 65
```

wireless wps auto-immune

To enable protection from Denial of Service (DoS) attacks, use the **wireless wps auto-immune** command. To disable, use the no form of the command.

wireless wps auto-immune

no wireless wps auto-immune

Command Default

Disabled.

Command Modes

config

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

A potential attacker can use specially crafted packets to mislead the Intrusion Detection System (IDS) into treating a legitimate client as an attacker. It causes the controller to disconnect this legitimate client and launch a DoS attack. The auto-immune feature, when enabled, is designed to protect against such attacks. However, conversations using Cisco 792x phones might be interrupted intermittently when the auto-immune feature is enabled. If you experience frequent disruptions when using 792x phones, you might want to disable this feature.

Examples

This example shows how to

```
Controller#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)#wireless wps auto-immune
```

wireless wps cids-sensor

To configure Intrusion Detection System (IDS) sensors for the Wireless Protection System (WPS), use the **wireless wps cids-sensor** command. To remove the Intrusion Detection System (IDS) sensors for the Wireless Protection System (WPS), use the no form of the command.

wireless wps cids-sensor *index* [**ip-address** *ip-addr* **username** *username* **password** *password_type password*]

no wireless wps cids-sensor *index*

Syntax Description

index	Specifies the IDS sensor internal index.
ip-address *ip-addr* **username** *username* **password** *password_type password*	Specifies the IDS sensor IP address, IDS sensor username, password type and IDS sensor password.

Command Default

Disabled.

Command Modes

config

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

None

Examples

This example shows how to configure the intrusion detection system with the IDS index, IDS sensor IP address, IDS username and IDS password.

```
Controller#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)#wireless wps cids-sensor 1 10.0.0.51 Sensor_user0doc1 passowrd01
```

wireless wps client-exclusion

To configure client exclusion policies, use the **wireless wps client-exclusion** command. To remove the client exclusion policies, use the no form of the command.

wireless wps client-exclusion {**all**| **dot11-assoc**| **dot11-auth**| **dot1x-auth**| **ip-theft**| **web-auth**}

no wireless wps client-exclusion {**all**| **dot11-assoc**| **dot11-auth**| **dot1x-auth**| **ip-theft**| **web-auth**}

Syntax Description

dot11-assoc	Specifies that the controller excludes clients on the sixth 802.11 association attempt, after five consecutive failures.
dot11-auth	Specifies that the controller excludes clients on the sixth 802.11 authentication attempt, after five consecutive failures.
dot1x-auth	Specifies that the controller excludes clients on the sixth 802.11X authentication attempt, after five consecutive failures.
ip-theft	Specifies that the control excludes clients if the IP address is already assigned to another device.
web-auth	Specifies that the controller excludes clients on the fourth web authentication attempt, after three consecutive failures.
all	Specifies that the controller excludes clients for all of the above reasons.

Command Default

Enabled.

Command Modes

config

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

None.

Examples

This example shows how to disable clients on the 802.11 association attempt after five consecutive failures.

```
Controller#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)#wireless wps client-exclusion dot11-assoc
```

wireless wps mfp infrastructure

To configure Management Frame Protection (MFP), use the **wireless wps mfp infrastructure** command. To remove the Management Frame Protection (MFP), use the no form of the command.

wireless wps mfp infrastructure

no wireless wps mfp infrastructure

Command Default

None.

Command Modes

config

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

None.

Examples

This example shows how to enable the infrastructure MFP.

```
Controller#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)#wireless wps mfp infrastructure
```

wireless wps rogue

To configure various rouge parameters, use the **wireless wps rogue** command.

wireless wps rogue {**adhoc**| **client**} [**alert** *mac-addr*| **contain** *mac-addr no-of-aps*]

Syntax Description

adhoc	Configures the status of an Independent Basic Service Set (IBSS or ad-hoc) rogue access point.
client	Configures rogue clients
alert *mac-addr*	Generates an SMNP trap upon detection of the ad-hoc rogue, and generates an immediate alert to the system administrator for further action for the MAC address of the ad-hoc rogue access point.
contain *mac-addr no-of-aps*	Contains the offending device so that its signals no longer interfere with authorized clients. Maximum number of Cisco access points assigned to actively contain the ad-hoc rogue access point (1 through 4, inclusive).

Command Default

None.

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

None.

Examples

This example shows how to generate an immediate alert to the system administrator for further action for the MAC address of the ad-hoc rogue access point.

```
Controller#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)#wireless wps rouge adhoc alert mac_addr
```

wireless wps shun-list re-sync

To force the controller to synchronization with other controllers in the mobility group for the shun list, use the **wireless wps shun-list re-sync** command.

wireless wps shun-list re-sync

Command Default

None.

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

None.

Examples

This example shows how to configure the controller to synchronize with other controllers for the shun list.

```
Controller#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)#wireless wps shun-list re-sync
```

vlan access-map

To create or modify a VLAN map entry for VLAN packet filtering, and change the mode to the VLAN access-map configuration, use the **vlan access-map** command in global configuration mode on the switch stack or on a standalone switch. To delete a VLAN map entry, use the **no** form of this command.

vlan access-map *name* [*number*]

no vlan access-map *name* [*number*]

Note This command is not supported on switches running the LAN Base feature set.

Syntax Description

name	Name of the VLAN map.
number	(Optional) The sequence number of the map entry that you want to create or modify (0 to 65535). If you are creating a VLAN map and the sequence number is not specified, it is automatically assigned in increments of 10, starting from 10. This number is the sequence to insert to, or delete from, a VLAN access-map entry.

Command Default

There are no VLAN map entries and no VLAN maps applied to a VLAN.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

In global configuration mode, use this command to create or modify a VLAN map. This entry changes the mode to VLAN access-map configuration, where you can use the **match** access-map configuration command to specify the access lists for IP or non-IP traffic to match and use the **action** command to set whether a match causes the packet to be forwarded or dropped.

In VLAN access-map configuration mode, these commands are available:

- **action—**Sets the action to be taken (forward or drop).
- **default—**Sets a command to its defaults.
- **exit—**Exits from VLAN access-map configuration mode.
- **match—**Sets the values to match (IP address or MAC address).

- **no—**Negates a command or set its defaults.

When you do not specify an entry number (sequence number), it is added to the end of the map.

There can be only one VLAN map per VLAN and it is applied as packets are received by a VLAN.

You can use the **no vlan access-map** *name* [*number*] command with a sequence number to delete a single entry.

Use the **vlan filter** interface configuration command to apply a VLAN map to one or more VLANs.

For more information about VLAN map entries, see the software configuration guide for this release.

Examples

This example shows how to create a VLAN map named vac1 and apply matching conditions and actions to it. If no other entries already exist in the map, this will be entry 10.

```
Controller(config)# vlan access-map vac1
Controller(config-access-map)# match ip address acl1
Controller(config-access-map)# action forward
```

This example shows how to delete VLAN map vac1:

```
Controller(config)# no vlan access-map vac1
```

Related Commands

Command	Description
action	Sets the action for the VLAN access map entry.
match (access-map configuration)	Sets the VLAN map to match packets against one or more access lists.
show vlan access-map	Displays the VLAN access maps created on the switch.
vlan filter	Applies a VLAN map to one or more VLANs.

vlan filter

To apply a VLAN map to one or more VLANs, use the **vlan filter** command in global configuration mode on the switch stack or on a standalone switch. To remove the map, use the **no** form of this command.

vlan filter *mapname* **vlan-list** {*list*| **all**}

no vlan filter *mapname* **vlan-list** {*list*| **all**}

Note This command is not supported on switches running the LAN Base feature set.

Syntax Description

mapname	Name of the VLAN map entry.
vlan-list	Specifies which VLANs to apply the map to.
list	The list of one or more VLANs in the form tt, uu-vv, xx, yy-zz, where spaces around commas and dashes are optional. The range is 1 to 4094.
all	Adds the map to all VLANs.

Command Default

There are no VLAN filters.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

To avoid accidentally dropping too many packets and disabling connectivity in the middle of the configuration process, we recommend that you completely define the VLAN access map before applying it to a VLAN.

For more information about VLAN map entries, see the software configuration guide for this release.

Examples

This example applies VLAN map entry map1 to VLANs 20 and 30:

```
Controller(config)# vlan filter map1 vlan-list 20, 30
```

This example shows how to delete VLAN map entry mac1 from VLAN 20:

```
Controller(config)# no vlan filter map1 vlan-list 20
```

You can verify your settings by entering the **show vlan filter** privileged EXEC command.

Related Commands

Command	Description
show vlan access-map	Displays the VLAN access maps created on the switch.
show vlan filter	Displays information about all VLAN filters or about a particular VLAN or VLAN access map.
vlan access-map	Defines a VLAN map and enters access-map configuration mode where you can specify a MAC ACL to match and the action to be taken.

vlan group

To create or modify a VLAN group, use the **vlan group** command in global configuration mode. To remove a VLAN list from the VLAN group, use the **no** form of this command.

vlan group *group-name* **vlan-list** *vlan-list*

no vlan group *group-name* **vlan-list** *vlan-list*

Syntax Description

group-name	Name of the VLAN group. The group name may contain up to 32 characters and must begin with a letter.
vlan-list *vlan-list*	Specifies one or more VLANs to be added to the VLAN group. The *vlan-list* argument can be a single VLAN ID, a list of VLAN IDs, or VLAN ID range. Multiple entries are separated by a hyphen (-) or a comma (,).

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

If the named VLAN group does not exist, the **vlan group** command creates the group and maps the specified VLAN list to the group. If the named VLAN group exists, the specified VLAN list is mapped to the group.

The **no** form of the **vlan group** command removes the specified VLAN list from the VLAN group. When you remove the last VLAN from the VLAN group, the VLAN group is deleted.

A maximum of 100 VLAN groups can be configured, and a maximum of 4094 VLANs can be mapped to a VLAN group.

Examples

This example shows how to map VLANs 7 through 9 and 11 to a VLAN group:

```
Controller(config)# vlan group group1 vlan-list 7-9,11
```

This example shows how to remove VLAN 7 from the VLAN group:

```
Controller(config)# no vlan group group1 vlan-list 7
```

Related Commands

Command	Description
show vlan group	Displays the VLANs mapped to VLAN groups.

PART VIII

Layer 2

Layer 2/3 Commands

- udld port, page 515
- udld reset, page 517

channel-group

To assign an Ethernet port to an EtherChannel group, to enable an EtherChannel mode, or both, use the **channel-group** command in interface configuration mode. To remove an Ethernet port from an EtherChannel group, use the **no** form of this command.

channel-group *channel-group-number* **mode** {**active**| **auto** [**non-silent**]| **desirable** [**non-silent**]| **on**| **passive**}

no channel-group

Syntax Description

channel-group-number	Channel group number. The range is 1 to 128.
mode	Specifies the EtherChannel mode.
active	Unconditionally enables Link Aggregation Control Protocol (LACP).
auto	Enables the Port Aggregation Protocol (PAgP) only if a PAgP device is detected.
non-silent	(Optional) Configures the interface for nonsilent operation when connected to a partner that is PAgP-capable. Use in PAgP mode with the **auto** or **desirable** keyword when traffic is expected from the other device.
desirable	Unconditionally enables PAgP.
on	Enables the on mode.
passive	Enables LACP only if a LACP device is detected.

Command Default

No channel groups are assigned.

No mode is configured.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

For Layer 2 EtherChannels, the **channel-group** command automatically creates the port-channel interface when the channel group gets its first physical port; therefore, you do not have to use the **interface port-channel** command in global configuration mode to manually create a port-channel interface. If you create the port-channel interface first, the *channel-group-number* can be the same as the *port-channel-number*, or you

can use a new number. If you use a new number, the **channel-group** command dynamically creates a new port channel.

You do not have to disable the IP address that is assigned to a physical port that is part of a channel group, but we strongly recommend that you do so.

You create Layer 3 port channels by using the **interface port-channel** command followed by the **no switchport** interface configuration command. Manually configure the port-channel logical interface before putting the interface into the channel group.

After you configure an EtherChannel, configuration changes that you make on the port-channel interface apply to all the physical ports assigned to the port-channel interface. Configuration changes applied to the physical port affect only the port where you apply the configuration. To change the parameters of all ports in an EtherChannel, apply configuration commands to the port-channel interface, for example, spanning-tree commands or commands to configure a Layer 2 EtherChannel as a trunk.

Active mode places a port into a negotiating state in which the port initiates negotiations with other ports by sending LACP packets. A channel is formed with another port group in either the active or passive mode.

Auto mode places a port into a passive negotiating state in which the port responds to PAgP packets it receives but does not start PAgP packet negotiation. A channel is formed only with another port group in desirable mode. When auto is enabled, silent operation is the default.

Desirable mode places a port into an active negotiating state in which the port starts negotiations with other ports by sending PAgP packets. An EtherChannel is formed with another port group that is in the desirable or auto mode. When desirable is enabled, silent operation is the default.

If you do not specify non-silent with the auto or desirable mode, silent is assumed. The silent mode is used when the controller is connected to a device that is not PAgP-capable and seldom, if ever, sends packets. A example of a silent partner is a file server or a packet analyzer that is not generating traffic. In this case, running PAgP on a physical port prevents that port from ever becoming operational. However, it allows PAgP to operate, to attach the port to a channel group, and to use the port for transmission. Both ends of the link cannot be set to silent.

In on mode, a usable EtherChannel exists only when both connected port groups are in the on mode.

Caution Use care when using the on mode. This is a manual configuration, and ports on both ends of the EtherChannel must have the same configuration. If the group is misconfigured, packet loss or spanning-tree loops can occur.

Passive mode places a port into a negotiating state in which the port responds to received LACP packets but does not initiate LACP packet negotiation. A channel is formed only with another port group in active mode.

Do not configure an EtherChannel in both the PAgP and LACP modes. EtherChannel groups running PAgP and LACP can coexist on the same controller or on different controller in the stack (but not in a cross-stack configuration). Individual EtherChannel groups can run either PAgP or LACP, but they cannot interoperate.

If you set the protocol by using the **channel-protocol** interface configuration command, the setting is not overridden by the **channel-group** interface configuration command.

Do not configure a port that is an active or a not-yet-active member of an EtherChannel as an IEEE 802.1x port. If you try to enable IEEE 802.1x authentication on an EtherChannel port, an error message appears, and IEEE 802.1x authentication is not enabled.

Do not configure a secure port as part of an EtherChannel or an EtherChannel port as a secure port.

For a complete list of configuration guidelines, see the “Configuring EtherChannels” chapter in the software configuration guide for this release.

Caution Do not enable Layer 3 addresses on the physical EtherChannel ports. Do not assign bridge groups on the physical EtherChannel ports because it creates loops.

Examples

This example shows how to configure an EtherChannel on a single controller in the stack. It assigns two static-access ports in VLAN 10 to channel 5 with the PAgP mode desirable:

```
Controller# configure terminal
Controller(config)# interface range gigabitethernet2/0/1 -2
Controller(config-if-range)# switchport mode access
Controller(config-if-range)# switchport access vlan 10
Controller(config-if-range)# channel-group 5 mode desirable
Controller(config-if-range)# end
```

This example shows how to configure an EtherChannel on a single controller in the stack. It assigns two static-access ports in VLAN 10 to channel 5 with the LACP mode active:

```
Controller# configure terminal
Controller(config)# interface range gigabitethernet2/0/1 -2
Controller(config-if-range)# switchport mode access
Controller(config-if-range)# switchport access vlan 10
Controller(config-if-range)# channel-group 5 mode active
Controller(config-if-range)# end
```

This example shows how to configure a cross-stack EtherChannel in a controller stack. It uses LACP passive mode and assigns two ports on stack member 2 and one port on stack member 3 as static-access ports in VLAN 10 to channel 5:

```
Controller# configure terminal
Controller(config)# interface range gigabitethernet2/0/4 -5
Controller(config-if-range)# switchport mode access
Controller(config-if-range)# switchport access vlan 10
Controller(config-if-range)# channel-group 5 mode passive
Controller(config-if-range)# exit
Controller(config)# interface gigabitethernet3/0/3
Controller(config-if)# switchport mode access
Controller(config-if)# switchport access vlan 10
Controller(config-if)# channel-group 5 mode passive
Controller(config-if)# exit
```

You can verify your settings by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
channel-protocol	Restricts the protocol used on a port to manage channeling.
interface port-channel	Accesses or creates a port channel.
show etherchannel	Displays EtherChannel information for a channel.
show lacp	Displays LACP channel-group information.
show pagp	Displays Port Aggregation Protocol (PAgP) channel-group information.

channel-protocol

To restrict the protocol used on a port to manage channeling, use the **channel-protocol** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

channel-protocol {**lacp**| **pagp**}

no channel-protocol

Syntax Description

lacp	Configures an EtherChannel with the Link Aggregation Control Protocol (LACP).
pagp	Configures an EtherChannel with the Port Aggregation Protocol (PAgP).

Command Default

No protocol is assigned to the EtherChannel.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Use the **channel-protocol** command only to restrict a channel to LACP or PAgP. If you set the protocol by using the **channel-protocol** command, the setting is not overridden by the **channel-group** interface configuration command.

You must use the **channel-group** interface configuration command to configure the EtherChannel parameters. The **channel-group** command also can set the mode for the EtherChannel.

You cannot enable both the PAgP and LACP modes on an EtherChannel group.

PAgP and LACP are not compatible; both ends of a channel must use the same protocol.

Examples

This example shows how to specify LACP as the protocol that manages the EtherChannel:

```
Controller(config-if)# channel-protocol lacp
```

You can verify your settings by entering the **show etherchannel** [*channel-group-number*]**protocol** privileged EXEC command.

Related Commands

Command	Description
channel-group	Assigns an Ethernet port to an EtherChannel group, or enables an EtherChannel mode, or both.

Command	Description
show etherchannel	Displays EtherChannel information for a channel.

clear lacp

To clear Link Aggregation Control Protocol (LACP) channel-group counters, use the **clear lacp** command in privileged EXEC mode.

clear lacp [*channel-group-number*] **counters**

Syntax Description

channel-group-number	(Optional) Channel group number. The range is 1 to 128.
counters	Clears traffic counters.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You can clear all counters by using the **clear lacp counters** command, or you can clear only the counters for the specified channel group by using the **clear lacp** *channel-group-number* **counters** command.

Examples

This example shows how to clear all channel-group information:

```
Controller# clear lacp counters
```

This example shows how to clear LACP traffic counters for group 4:

```
Controller# clear lacp 4 counters
```

You can verify that the information was deleted by entering the **show lacp counters** or the **show lacp** *channel-group-number* **counters** privileged EXEC command.

Related Commands

Command	Description
show lacp	Displays LACP channel-group information.

clear pagp

To clear the Port Aggregation Protocol (PAgP) channel-group information, use the **clear pagp** command in privileged EXEC mode.

clear pagp [*channel-group-number*] **counters**

Syntax Description

channel-group-number	(Optional) Channel group number. The range is 1 to 128.
counters	Clears traffic counters.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You can clear all counters by using the **clear pagp counters** command, or you can clear only the counters for the specified channel group by using the **clear pagp** *channel-group-number* **counters** command.

Examples

This example shows how to clear all channel-group information:

```
Controller# clear pagp counters
```

This example shows how to clear PAgP traffic counters for group 10:

```
Controller# clear pagp 10 counters
```

You can verify that the information was deleted by entering the **show pagp** privileged EXEC command.

Related Commands

Command	Description
show pagp	Displays Port Aggregation Protocol (PAgP) channel-group information.

debug platform pm

To enable debugging of the platform-dependent port manager software module, use the **debug platform pm** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug platform pm {**all**| **counters**| **errdisable**| **fec**| **if-numbers**| **l2-control**| **link-status**| **platform**| **pm-spi**| **pm-vectors [detail]**| **ses**| **vlans**}

no debug platform pm {**all**| **counters**| **errdisable**| **fec**| **if-numbers**| **l2-control**| **link-status**| **platform**| **pm-spi**| **pm-vectors [detail]**| **ses**| **vlans**}

Syntax Description

all	Displays all port manager debug messages.
counters	Displays counters for remote procedure call (RPC) debug messages.
errdisable	Displays error-disabled-related events debug messages.
fec	Displays forwarding equivalence class (FEC) platform-related events debug messages.
if-numbers	Displays interface-number translation event debug messages.
l2-control	Displays Layer 2 control infra debug messages.
link-status	Displays interface link-detection event debug messages.
platform	Displays port manager function event debug messages.
pm-spi	Displays port manager stateful packet inspection (SPI) event debug messages.
pm-vectors	Displays port manager vector-related event debug messages.
detail	(Optional) Displays vector-function details.
ses	Displays service expansion shelf (SES) related event debug messages.
ses	Displays service expansion shelf (SES) related event debug messages.
vlans	Displays VLAN creation and deletion event debug messages.

Command Default

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The **undebug platform pm** command is the same as the **no debug platform pm** command.

debug platform udld

To enable debugging of the platform-dependent UniDirectional Link Detection (UDLD) software, use the **debug platform udld** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug platform udld [**error**| **event**] [**switch** *switch-number*]

no debug platform udld [**error**| **event**] [**switch** *switch-number*]

Syntax Description

error	(Optional) Displays error condition debug messages.
event	(Optional) Displays UDLD related platform event debug messages.
switch *switch-number*	(Optional) Displays UDLD debug messages for the specified stack member.

Command Default

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The **undebug platform udld** command is the same as the **no debug platform udld** command.

interface port-channel

To access or create a port-channel, use the **interface port-channel** command in global configuration mode. Use the **no** form of this command to remove the port channel.

interface port-channel *port-channel-number*

Syntax Description

port-channel-number	Port-channel number. The range is 1 to 128.

Command Default

No port channel logical interfaces are defined.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

For Layer 2 EtherChannels, you do not have to create a port-channel interface before assigning physical ports to a channel group. Instead, you can use the **channel-group** interface configuration command, which automatically creates the port-channel interface when the channel group gets its first physical port. If you create the port-channel interface first, the *channel-group-number* can be the same as the *port-channel-number*, or you can use a new number. If you use a new number, the **channel-group** command dynamically creates a new port channel.

You create Layer 3 port channels by using the **interface port-channel** command followed by the **no switchport** interface configuration command. You should manually configure the port-channel logical interface before putting the interface into the channel group.

Only one port channel in a channel group is allowed.

Caution When using a port-channel interface as a routed port, do not assign Layer 3 addresses on the physical ports that are assigned to the channel group.

Caution Do not assign bridge groups on the physical ports in a channel group used as a Layer 3 port channel interface because it creates loops. You must also disable spanning tree.

Follow these guidelines when you use the **interface port-channel** command:

- If you want to use the Cisco Discovery Protocol (CDP), you must configure it on the physical port and not on the port channel interface.

- Do not configure a port that is an active member of an EtherChannel as an IEEE 802.1x port. If IEEE 802.1x is enabled on a not-yet active port of an EtherChannel, the port does not join the EtherChannel.

For a complete list of configuration guidelines, see the "Configuring EtherChannels" chapter in the software configuration guide for this release.

Examples

This example shows how to create a port channel interface with a port channel number of 5:

```
Controller(config)# interface port-channel 5
```

You can verify your setting by entering the **show running-config** privileged EXEC or **show etherchannel** *channel-group-number* **detail** privileged EXEC command.

Related Commands

Command	Description
channel-group	Assigns an Ethernet port to an EtherChannel group, or enables an EtherChannel mode, or both.
show etherchannel	Displays EtherChannel information for a channel.

lacp port-priority

To configure the port priority for the Link Aggregation Control Protocol (LACP), use the **lacp port-priority** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

lacp port-priority *priority*

no lacp port-priority

Syntax Description

priority	Port priority for LACP. The range is 1 to 65535.

Command Default

The default is 32768.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The **lacp port-priority** interface configuration command determines which ports are bundled and which ports are put in hot-standby mode when there are more than eight ports in an LACP channel group.

An LACP channel group can have up to 16 Ethernet ports of the same type. Up to eight ports can be active, and up to eight ports can be in standby mode.

In port-priority comparisons, a numerically *lower* value has a *higher* priority: When there are more than eight ports in an LACP channel group, the eight ports with the numerically lowest values (highest priority values) for LACP port priority are bundled into the channel group, and the lower-priority ports are put in hot-standby mode. If two or more ports have the same LACP port priority (for example, they are configured with the default setting of 65535), then an internal value for the port number determines the priority.

Note The LACP port priorities are only effective if the ports are on the controller that controls the LACP link. See the **lacp system-priority** global configuration command for determining which controller controls the link.

Use the **show lacp internal** privileged EXEC command to display LACP port priorities and internal port number values.

For information about configuring LACP on physical ports, see the configuration guide for this release.

Examples

This example shows how to configure the LACP port priority on a port:

```
Controller# interface gigabitethernet2/0/1
Controller(config-if)# lacp port-priority 1000
```

You can verify your settings by entering the **show lacp** [*channel-group-number*] **internal** privileged EXEC command.

Related Commands

Command	Description
channel-group	Assigns an Ethernet port to an EtherChannel group, or enables an EtherChannel mode, or both.
lacp system-priority	Configures the LACP system priority.
show lacp	Displays LACP channel-group information.

lacp system-priority

To configure the system priority for the Link Aggregation Control Protocol (LACP), use the **lacp system-priority** command in global configuration mode on the controller. To return to the default setting, use the **no** form of this command.

lacp system-priority *priority*

no lacp system-priority

Syntax Description

priority	System priority for LACP. The range is 1 to 65535.

Command Default

The default is 32768.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The **lacp system-priority** command determines which controller in an LACP link controls port priorities.

An LACP channel group can have up to 16 Ethernet ports of the same type. Up to eight ports can be active, and up to eight ports can be in standby mode. When there are more than eight ports in an LACP channel group, the controller on the controlling end of the link uses port priorities to determine which ports are bundled into the channel and which ports are put in hot-standby mode. Port priorities on the other controller (the noncontrolling end of the link) are ignored.

In priority comparisons, numerically lower values have higher priority. Therefore, the system with the numerically lower value (higher priority value) for LACP system priority becomes the controlling system. If both controller have the same LACP system priority (for example, they are both configured with the default setting of 32768), the LACP system ID (the controller MAC address) determines which controller is in control.

The **lacp system-priority** command applies to all LACP EtherChannels on the controller.

Use the **show etherchannel summary** privileged EXEC command to see which ports are in the hot-standby mode (denoted with an H port-state flag in the output display).

Examples

This example shows how to set the LACP system priority:

```
Controller(config)# lacp system-priority 20000
```

You can verify your settings by entering the **show lacp sys-id** privileged EXEC command.

Related Commands

Command	Description
channel-group	Assigns an Ethernet port to an EtherChannel group, or enables an EtherChannel mode, or both.
lacp port-priority	Configures the port priority for the Link Aggregation Control Protocol (LACP).
show lacp	Displays LACP channel-group information.

pagp learn-method

To learn the source address of incoming packets received from an EtherChannel port, use the **pagp learn-method** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

pagp learn-method {**aggregation-port**| **physical-port**}

no pagp learn-method

Syntax Description

aggregation-port	Specifies address learning on the logical port channel. The controller sends packets to the source using any port in the EtherChannel. This setting is the default. With aggregation-port learning, it is not important on which physical port the packet arrives.
physical-port	Specifies address learning on the physical port within the EtherChannel. The controller sends packets to the source using the same port in the EtherChannel from which it learned the source address. The other end of the channel uses the same port in the channel for a particular destination MAC or IP address.

Command Default

The default is aggregation-port (logical port channel).

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The learn method must be configured the same at both ends of the link.

The controller supports address learning only on aggregate ports even though the **physical-port** keyword is provided in the command-line interface (CLI). The **pagp learn-method** and the **pagp port-priority** interface configuration commands have no effect on the controller hardware, but they are required for PAgP interoperability with devices that only support address learning by physical ports. .

When the link partner to the controller is a physical learner, we recommend that you configure the controller as a physical-port learner by using the **pagp learn-method physical-port** interface configuration command and to set the load-distribution method based on the source MAC address by using the **port-channel load-balance src-mac** global configuration command. Use the **pagp learn-method** interface configuration command only in this situation.

Examples

This example shows how to set the learning method to learn the address on the physical port within the EtherChannel:

```
Controller(config-if)# pagp learn-method physical-port
```

This example shows how to set the learning method to learn the address on the port channel within the EtherChannel:

```
Controller(config-if)# pagp learn-method aggregation-port
```

You can verify your settings by entering the **show running-config** privileged EXEC command or the **show pagp** *channel-group-number* **internal** privileged EXEC command.

Related Commands

Command	Description
pagp port-priority	Selects a port over which all traffic through the EtherChannel is sent.
show pagp	Displays Port Aggregation Protocol (PAgP) channel-group information.

pagp port-priority

To select a port over which all Port Aggregation Protocol (PAgP) traffic through the EtherChannel is sent, use the **pagp port-priority** command in interface configuration mode. If all unused ports in the EtherChannel are in hot-standby mode, they can be placed into operation if the currently selected port and link fails. To return to the default setting, use the **no** form of this command.

pagp port-priority *priority*

no pagp port-priority

Syntax Description

priority	Priority number. The range is from 0 to 255.

Command Default

The default is 128.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The physical port with the highest priority that is operational and has membership in the same EtherChannel is the one selected for PAgP transmission.

The controller supports address learning only on aggregate ports even though the **physical-port** keyword is provided in the command-line interface (CLI). The **pagp learn-method** and the **pagp port-priority** interface configuration commands have no effect on the controller hardware, but they are required for PAgP interoperability with devices that only support address learning by physical ports, such as the Catalyst 1900 switch.

When the link partner to the controller is a physical learner, we recommend that you configure the controller as a physical-port learner by using the **pagp learn-method physical-port** interface configuration command and to set the load-distribution method based on the source MAC address by using the **port-channel load-balance src-mac** global configuration command. Use the **pagp learn-method** interface configuration command only in this situation.

Examples

This example shows how to set the port priority to 200:

```
Controller(config-if)# pagp port-priority 200
```

You can verify your setting by entering the **show running-config** privileged EXEC command or the **show pagp** *channel-group-number* **internal** privileged EXEC command.

Related Commands

Command	Description
pagp learn-method	Provides the ability to learn the source address of incoming packets.
port-channel load-balance	Sets the load-distribution method among the ports in the EtherChannel.
show pagp	Displays Port Aggregation Protocol (PAgP) channel-group information.

port-channel load-balance

To set the load-distribution method among the ports in the EtherChannel, use the **port-channel load-balance** command in global configuration mode. To reset the load balancing mechanism to the default setting, use the **no** form of this command.

no port-channel load-balance

Syntax Description

dst-ip	Specifies load distribution based on the destination host IP address.
dst-mac	Specifies load distribution based on the destination host MAC address. Packets to the same destination are sent on the same port, but packets to different destinations are sent on different ports in the channel.
src-dst-ip	Specifies load distribution based on the source and destination host IP address.
src-dst-mac	Specifies load distribution based on the source and destination host MAC address.
src-ip	Specifies load distribution based on the source host IP address.
src-mac	Specifies load distribution based on the source MAC address. Packets from different hosts use different ports in the channel, but packets from the same host use the same port.

Command Default

The default is **src-mac**.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You can verify your setting by entering the **show running-config** privileged EXEC command or the **show etherchannel load-balance** privileged EXEC command.

Examples

This example shows how to set the load-distribution method to **dst-mac**:

```
Controller(config)# port-channel load-balance dst-mac
```

Related Commands

Command	Description
port-channel load-balance extended	Sets extended load-distribution methods among the ports in the EtherChannel.

port-channel load-balance extended

To set extended load-distribution methods among the ports in the EtherChannel, use the **port-channel load-balance extended** command in global configuration mode. To reset the extended load balancing mechanism to the default setting, use the **no** form of this command.

port-channel load-balance extended [**dst-ip**] [**dst-mac**] [**dst-port**] [**ipv6-label**] [**l3-proto**] [**src-ip**] [**src-mac**] [**src-port**]

no port-channel load-balance extended

Syntax Description

dst-ip	(Optional) Specifies load distribution based on the destination host IP address.
dst-mac	(Optional) Specifies load distribution based on the destination host MAC address. Packets to the same destination are sent on the same port, but packets to different destinations are sent on different ports in the channel.
dst-port	(Optional) Specifies load distribution based on the destination TCP/UDP (Layer 4) port number for both IPv4 and IPv6.
ipv6-label	(Optional) Specifies load distribution based on the source MAC address and IPv6 flow label.
l3-proto	(Optional) Specifies load distribution based on the source MAC address and Layer 3 protocols.
src-ip	(Optional) Specifies load distribution based on the source host IP address.
src-mac	(Optional) Specifies load distribution based on the source MAC address. Packets from different hosts use different ports in the channel, but packets from the same host use the same port.
src-port	(Optional) Specifies load distribution based on the TCP/UDP (Layer 4) port number.

Command Default

The default is **src-mac**.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

For information about when to use these forwarding methods, see the *Layer 2 Configuration Guide (Cisco WLC 5700 Series)* for this release.

You can verify your setting by entering the **show running-config** privileged EXEC command or the **show etherchannel load-balance** privileged EXEC command.

Examples

This example shows how to set the extended load-distribution method to dst-port:

```
Controller(config)# port-channel load-balance extended dst-port
```

Related Commands

Command	Description
port-channel load-balance	Sets the load-distribution method among the ports in the EtherChannel.

show etherchannel

To display EtherChannel information for a channel, use the **show etherchannel** command in user EXEC mode.

show etherchannel [*channel-group-number* {**detail**| **port**| **port-channel**| **protocol**| **summary**}] {**detail**| **load-balance**| **port**| **port-channel**| **protocol**| **summary**}

Syntax Description

channel-group-number	(Optional) Channel group number. The range is 1 to 128.
detail	Displays detailed EtherChannel information.
load-balance	Displays the load-balance or frame-distribution scheme among ports in the port channel.
port	Displays EtherChannel port information.
port-channel	Displays port-channel information.
protocol	Displays the protocol that is being used in the channel.
summary	Displays a one-line summary per channel group.

Command Default

None

Command Modes

User EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

If you do not specify a **channel-group**, all channel groups are displayed.

In the output, the Passive port list field is displayed only for Layer 3 port channels. This field means that the physical port, which is still not up, is configured to be in the channel group (and indirectly is in the only port channel in the channel group).

Note Layer 3 port channels are not supported when the controller is running the LAN Base feature set.

Examples

This is an example of output from the **show etherchannel** *channel-group-number* **detail** command:

```
Controller> show etherchannel 1 detail
Group state = L2
Ports: 2   Maxports = 16
Port-channels: 1 Max Port-channels = 16
Protocol:      LACP
                   Ports in the group:
                   -------------------
Port: Gi1/0/1
------------
Port state    = Up Mstr In-Bndl
Channel group = 1        Mode  = Active        Gcchange = -
Port-channel  =          Po1GC = -             Pseudo port-channel = Po1
Port index    =          0Load = 0x00          Protocol = LACP

Flags: S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDU
       A - Device is in active mode.        P - Device is in passive mode.

Local information:
                         LACP port   Admin   Oper   Port   Port
Port     Flags   State   Priority    Key     Key    Number State
Gi1/0/1   SA      bndl     32768      0x1     0x1    0x101  0x3D
Gi1/0/2    A      bndl     32768      0x0     0x1    0x0    0x3D

Age of the port in the current state: 01d:20h:06m:04s

                   Port-channels in the group:
                   ----------------------

Port-channel: Po1   (Primary Aggregator)

Age of the Port-channel = 01d:20h:20m:26s
Logical slot/port = 10/1          Number of ports = 2
HotStandBy port   = null
Port state        = Port-channel Ag-Inuse
Protocol          = LACP

Ports in the Port-channel:

Index  Load   Port      EC state        No of bits
------+------+------+------------------+-----------
 0      00    Gi1/0/1    Active           0
 0      00    Gi1/0/2    Active           0

Time since last port bundled:   01d:20h:24m:44s   Gi1/0/2
```

This is an example of output from the **show etherchannel** *channel-group-number* **summary** command:

```
Controller> show etherchannel 1 summary
Flags: D - down P - in port-channel
       I - stand-alone s - suspended
       H - Hot-standby (LACP only)
       R - Layer3 S - Layer2
       u - unsuitable for bundling
       U - in use f - failed to allocate aggregator
       d - default port

Number of channel-groups in use: 1
Number of aggregators: 1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------
 1     Po1(SU)       LACP        Gi1/0/1(P) Gi1/0/2(P)
```

This is an example of output from the **show etherchannel** *channel-group-number* **port-channel** command:

```
Controller> show etherchannel 1 port-channel
Port-channels in the group:
----------------------
```

```
Port-channel: Po1 (Primary Aggregator)
------------
Age of the Port-channel = 01d:20h:24m:50s
Logical slot/port = 10/1 Number of ports = 2
Logical slot/port = 10/1 Number of ports = 2
Port state = Port-channel Ag-Inuse
Protocol = LACP

Ports in the Port-channel:

Index  Load   Port   EC state           No of bits
------+------+------+------------------+-----------
 0      00    Gi1/0/1 Active             0
 0      00    Gi1/0/2 Active             0

Time since last port bundled: 01d:20h:24m:44s Gi1/0/2
```

This is an example of output from **show etherchannel protocol** command:

```
Controller# show etherchannel protocol
Channel-group listing:
----------------------
Group: 1
----------
Protocol: LACP
Group: 2
----------
Protocol: PAgP
```

Related Commands

Command	Description
channel-group	Assigns an Ethernet port to an EtherChannel group, or enables an EtherChannel mode, or both.
channel-protocol	Restricts the protocol used on a port to manage channeling.
interface port-channel	Accesses or creates a port channel.

show lacp

To display Link Aggregation Control Protocol (LACP) channel-group information, use the **show lacp** command in user EXEC mode.

show lacp [*channel-group-number*] {**counters**| **internal**| **neighbor**| **sys-id**}

Syntax Description

channel-group-number	(Optional) Channel group number. The range is 1 to 128.
counters	Displays traffic information.
internal	Displays internal information.
neighbor	Displays neighbor information.
sys-id	Displays the system identifier that is being used by LACP. The system identifier is made up of the LACP system priority and the controller MAC address.

Command Default

None

Command Modes

User EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You can enter any **show lacp** command to display the active channel-group information. To display specific channel information, enter the **show lacp** command with a channel-group number.

If you do not specify a channel group, information for all channel groups appears.

You can enter the *channel-group-number* to specify a channel group for all keywords except **sys-id**.

Examples

This is an example of output from the **show lacp counters** user EXEC command. The table that follows describes the fields in the display.

```
Controller> show lacp counters
              LACPDUs         Marker     Marker Response   LACPDUs
Port        Sent  Recv     Sent  Recv     Sent  Recv     Pkts  Err
--------------------------------------------------------------------
Channel group:1
Gi2/0/1      19    10        0    0         0    0        0
Gi2/0/2      14    6         0    0         0    0        0
```

Table 17: show lacp counters Field Descriptions

Field	Description
LACPDUs Sent and Recv	The number of LACP packets sent and received by a port.
Marker Sent and Recv	The number of LACP marker packets sent and received by a port.
Marker Response Sent and Recv	The number of LACP marker response packets sent and received by a port.
LACPDUs Pkts and Err	The number of unknown and illegal packets received by LACP for a port.

This is an example of output from the **show lacp internal** command:

```
Controller> show lacp 1 internal
Flags:  S - Device is requesting Slow LACPDUs
        F - Device is requesting Fast LACPDUs
        A - Device is in Active mode       P - Device is in Passive mode

Channel group 1
                            LACP port    Admin    Oper    Port     Port
Port      Flags   State     Priority     Key      Key     Number   State
Gi2/0/1    SA      bndl      32768         0x3      0x3       0x4    0x3D
Gi2/0/2    SA      bndl      32768         0x3      0x3       0x5    0x3D
```

The following table describes the fields in the display:

Table 18: show lacp internal Field Descriptions

Field	Description
State	State of the specific port. These are the allowed values: • **– —**Port is in an unknown state. • **bndl—**Port is attached to an aggregator and bundled with other ports. • **susp—**Port is in a suspended state; it is not attached to any aggregator. • **hot-sby—**Port is in a hot-standby state. • **indiv—**Port is incapable of bundling with any other port. • **indep—**Port is in an independent state (not bundled but able to handle data traffic. In this case, LACP is not running on the partner port). • **down—**Port is down.
LACP Port Priority	Port priority setting. LACP uses the port priority to put ports in standby mode when there is a hardware limitation that prevents all compatible ports from aggregating.
Admin Key	Administrative key assigned to this port. LACP automatically generates an administrative key value as a hexadecimal number. The administrative key defines the ability of a port to aggregate with other ports. A port's ability to aggregate with other ports is determined by the port physical characteristics (for example, data rate and duplex capability) and configuration restrictions that you establish.
Oper Key	Runtime operational key that is being used by this port. LACP automatically generates this value as a hexadecimal number.
Port Number	Port number.

Field	Description
Port State	State variables for the port, encoded as individual bits within a single octet with these meanings: • bit0: LACP_Activity • bit1: LACP_Timeout • bit2: Aggregation • bit3: Synchronization • bit4: Collecting • bit5: Distributing • bit6: Defaulted • bit7: Expired **Note** In the list above, bit7 is the MSB and bit0 is the LSB.

This is an example of output from the **show lacp neighbor** command:

```
Controller> show lacp neighbor
Flags: S - Device is sending Slow LACPDUs  F - Device is sending Fast LACPDUs
       A - Device is in Active mode        P - Device is in Passive mode

Channel group 3 neighbors

Partner's information:

          Partner                 Partner                 Partner
Port      System ID               Port Number   Age       Flags
Gi2/0/1   32768,0007.eb49.5e80    0xC             19s       SP

          LACP Partner            Partner       Partner
          Port Priority           Oper Key      Port State
          32768                   0x3           0x3C

Partner's information:

          Partner                 Partner                 Partner
Port      System ID               Port Number   Age       Flags
Gi2/0/2   32768,0007.eb49.5e80    0xD             15s       SP

          LACP Partner            Partner       Partner
          Port Priority           Oper Key      Port State
          32768                   0x3           0x3C
```

This is an example of output from the **show lacp sys-id** command:

```
Controller> show lacp sys-id
32765,0002.4b29.3a00
```

The system identification is made up of the system priority and the system MAC address. The first two bytes are the system priority, and the last six bytes are the globally administered individual MAC address associated to the system.

Related Commands

Command	Description
clear lacp	Clears the LACP channel-group information.
lacp port-priority	Configures the port priority for the Link Aggregation Control Protocol (LACP).
lacp system-priority	Configures the LACP system priority.

show pagp

To display Port Aggregation Protocol (PAgP) channel-group information, use the **show pagp** command in EXEC mode.

show pagp [*channel-group-number*] {**counters**| **dual-active**| **internal**| **neighbor**}

Syntax Description

channel-group-number	(Optional) Number of the channel group. The range is 1 to 128.
counters	Displays traffic information.
dual-active	Displays the dual-active status.
internal	Displays internal information.
neighbor	Displays neighbor information.

Command Default

None

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You can enter any **show pagp** command to display the active channel-group information. To display the nonactive information, enter the **show pagp** command with a channel-group number.

Examples

This is an example of output from the **show pagp 1 counters** command:

```
Controller> show pagp 1 counters
             Information        Flush
Port         Sent   Recv     Sent   Recv
---------------------------------------
Channel group: 1
  Gi1/0/1    45     42       0      0
  Gi1/0/2    45     41       0      0
```

This is an example of output from the **show pagp dual-active** command:

```
Controller> show pagp dual-active
PAgP dual-active detection enabled: Yes
PAgP dual-active version: 1.1
```

```
Channel group 1
          Dual-Active     Partner              Partner   Partner
Port      Detect Capable  Name                 Port      Version
Gi1/0/1   No              Switch               Gi3/0/3   N/A
Gi1/0/2   No              Switch               Gi3/0/4   N/A

<output truncated>
```

This is an example of output from the **show pagp 1 internal** command:

```
Controller> show pagp 1 internal
Flags:  S - Device is sending Slow hello.  C - Device is in Consistent state.
        A - Device is in Auto mode.
Timers: H - Hello timer is running.        Q - Quit timer is running.
        S - Switching timer is running.    I - Interface timer is running.

Channel group 1
                                Hello    Partner  PAgP     Learning  Group
Port        Flags State   Timers  Interval Count   Priority   Method  Ifindex
Gi1/0/1     SC    U6/S7   H       30s      1        128        Any      16
Gi1/0/2     SC    U6/S7   H       30s      1        128        Any      16
```

This is an example of output from the **show pagp 1 neighbor** command:

```
Controller> show pagp 1 neighbor

Flags:  S - Device is sending Slow hello.  C - Device is in Consistent state.
        A - Device is in Auto mode.        P - Device learns on physical port.

Channel group 1 neighbors
            Partner             Partner          Partner           Partner Group
Port        Name                Device ID        Port         Age  Flags   Cap.
Gi1/0/1     switch-p2           0002.4b29.4600   Gi01//1        9s SC      10001
Gi1/0/2     switch-p2           0002.4b29.4600   Gi1/0/2       24s SC      10001
```

Related Commands

Command	Description
clear pagp	Clears PAgP channel-group information.

show platform etherchannel

To display platform-dependent EtherChannel information, use the **show platform etherchannel** command in privileged EXEC mode.

show platform etherchannel *channel-group-number* {**group-mask**| **load-balance mac** *src-mac dst-mac* [**ip** *src-ip dst-ip* [**port** *src-port dst-port*]]} [**switch** *switch-number*]

Syntax Description

channel-group-number	Channel group number. The range is 1 to 128.
group-mask	Displays EtherChannel group mask.
load-balance	Tests EtherChannel load-balance hash algorithm.
mac *src-mac dst-mac*	Specifies the source and destination MAC addresses.
ip *src-ip dst-ip*	(Optional) Specifies the source and destination IP addresses.
port *src-port dst-port*	(Optional) Specifies the source and destination layer port numbers.
switch *switch-number*	(Optional) Specifies the stack member.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Use this command only when you are working directly with a technical support representative while troubleshooting a problem. Do not use this command unless a technical support representative asks you to do so.

show platform pm

To display platform-dependent port manager information, use the **show platform pm** command in privileged EXEC mode.

show platform pm {**etherchannel** *channel-group-number* **group-mask**| **interface-numbers**| **port-data** *interface-id*| **port-state**| **spi-info**| **spi-req-q**}

Syntax Description

etherchannel *channel-group-number* **group-mask**	Displays the etherchannel group-mask table for the specified channel-group. The channel-group range is 1 to 128.
interface-numbers	Displays interface numbers information.
port-data *interface-id*	Displays port data information for the specified interface.
port-state	Displays port state information.
spi-info	Displays stateful packet inspection (SPI) information.
spi-req-q	Displays stateful packet inspection (SPI) maximum wait time for acknowledgment.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Use this command only when you are working directly with your technical support representative while troubleshooting a problem. Do not use this command unless your technical support representative asks you to do so.

show udld

To display UniDirectional Link Detection (UDLD) administrative and operational status for all ports or the specified port, use the **show udld** command in user EXEC mode.

show udld [*interface-id*| **neighbors**]

Syntax Description

interface-id	(Optional) ID of the interface and port number. Valid interfaces include physical ports and VLANs. The range is 1 to 4094.
neighbors	(Optional) Displays neighbor information only.

Command Default

None

Command Modes

User EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

If you do not enter an interface ID, administrative and operational UDLD status for all interfaces appear.

Examples

This is an example of output from the **show udld** *interface-id* command. For this display, UDLD is enabled on both ends of the link, and UDLD detects that the link is bidirectional. The table that follows describes the fields in this display.

```
Controller> show udld gigabitethernet2/0/1
Interface gi2/0/1
---
Port enable administrative configuration setting: Follows device default
Port enable operational state: Enabled
Current bidirectional state: Bidirectional
Current operational state: Advertisement - Single Neighbor detected
Message interval: 60
Time out interval: 5
Entry 1
Expiration time: 146
Device ID: 1
Current neighbor state: Bidirectional
Device name: Switch-A
Port ID: Gi2/0/1
Neighbor echo 1 device: Switch-B
Neighbor echo 1 port: Gi2/0/2
Message interval: 5
CDP Device name: Switch-A
```

Table 19: show udld Field Descriptions

Field	Description
Interface	The interface on the local device configured for UDLD.
Port enable administrative configuration setting	How UDLD is configured on the port. If UDLD is enabled or disabled, the port enable configuration setting is the same as the operational enable state. Otherwise, the enable operational setting depends on the global enable setting.
Port enable operational state	Operational state that shows whether UDLD is actually running on this port.
Current bidirectional state	The bidirectional state of the link. An unknown state appears if the link is down or if it is connected to an UDLD-incapable device. A bidirectional state appears if the link is a normal two-way connection to a UDLD-capable device. All other values mean miswiring.
Current operational state	The current phase of the UDLD state machine. For a normal bidirectional link, the state machine is most often in the Advertisement phase.
Message interval	How often advertisement messages are sent from the local device. Measured in seconds.
Time out interval	The time period, in seconds, that UDLD waits for echoes from a neighbor device during the detection window.
Entry 1	Information from the first cache entry, which contains a copy of echo information received from the neighbor.
Expiration time	The amount of time in seconds remaining before this cache entry is aged out.
Device ID	The neighbor device identification.
Current neighbor state	The neighbor's current state. If both the local and neighbor devices are running UDLD normally, the neighbor state and local state should be bidirectional. If the link is down or the neighbor is not UDLD-capable, no cache entries appear.

Field	Description
Device name	The device name or the system serial number of the neighbor. The system serial number appears if the device name is not set or is set to the default (Switch).
Port ID	The neighbor port ID enabled for UDLD.
Neighbor echo 1 device	The device name of the neighbors' neighbor from which the echo originated.
Neighbor echo 1 port	The port number ID of the neighbor from which the echo originated.
Message interval	The rate, in seconds, at which the neighbor is sending advertisement messages.
CDP device name	The CDP device name or the system serial number. The system serial number appears if the device name is not set or is set to the default (Switch).

This is an example of output from the **show udld neighbors** command:

```
Controller# show udld neighbors
Port     Device Name          Device ID  Port-ID  OperState
-------- -------------------- ---------- -------- --------------
Gi2/0/1  Switch-A             1          Gi2/0/1  Bidirectional
Gi3/0/1  Switch-A             2          Gi3/0/1  Bidirectional
```

Related Commands

Command	Description
udld	Enables aggressive or normal mode in UDLD or sets the configurable message timer time.
udld port	Enables UDLD on an individual interface or prevents a fiber-optic interface from being enabled by the **udld** global configuration command.
udld reset	Resets all interfaces shut down by UDLD and permits traffic to pass through again.

switchport

To put an interface that is in Layer 3 mode into Layer 2 mode for Layer 2 configuration, use the **switchport** command in interface configuration mode. To put an interface in Layer 3 mode, use the **no** form of this command.

switchport

no switchport

Syntax Description

This command has no keywords or arguments.

Command Default

By default, all interfaces are in Layer 2 mode.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Use the **no switchport** command (without parameters) to set the interface to the routed-interface status and to erase all Layer 2 configurations. You must use this command before assigning an IP address to a routed port.

Note This command is not supported on controllers running the LAN Base feature set.

Entering the **no switchport** command shuts the port down and then reenables it, which might generate messages on the device to which the port is connected.

When you put an interface that is in Layer 2 mode into Layer 3 mode (or the reverse), the previous configuration information related to the affected interface might be lost, and the interface is returned to its default configuration.

Note If an interface is configured as a Layer 3 interface, you must first enter the **switchport** command to configure the interface as a Layer 2 port. Then you can enter the **switchport access vlan** and **switchport mode** commands.

The **switchport** command is not used on platforms that do not support Cisco-routed ports. All physical ports on such platforms are assumed to be Layer 2-switched interfaces.

You can verify the controller port status of an interface by entering the **show running-config** privileged EXEC command.

Examples

This example shows how to cause an interface to cease operating as a Layer 2 port and become a Cisco-routed port:

```
Controller(config-if)# no switchport
```

This example shows how to cause the port interface to cease operating as a Cisco-routed port and convert to a Layer 2 switched interface:

```
Controller(config-if)# switchport
```

switchport access vlan

To configure a port as a static-access, use the **switchport access vlan** command in interface configuration mode. To reset the access mode to the default VLAN mode for the controller, use the **no** form of this command.

switchport access vlan {*vlan-id*| **dynamic**}

no switchport access vlan

Syntax Description

vlan-id	VLAN ID of the access mode VLAN; the range is 1 to 4094.
dynamic	Specifies that the access mode VLAN is dependent on the VLAN Membership Policy Server (VMPS) protocol. The port is assigned to a VLAN based on the source MAC address of a host (or hosts) connected to the port. The switch sends every new MAC address received to the VMPS server to get the VLAN name to which the dynamic-access port should be assigned. If the port already has a VLAN assigned and the source has already been approved by the VMPS, the switch forwards the packet to the VLAN.

Command Default

The default access VLAN and trunk interface native VLAN is a default VLAN corresponding to the platform or interface hardware.

A dynamic-access port is initially a member of no VLAN and receives its assignment based on the packet it receives.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The port must be in access mode before the **switchport access vlan** command can take effect.

If the switchport mode is set to **access vlan** *vlan-id*, the port operates as a member of the specified VLAN. If set to **access vlan dynamic**, the port starts discovery of VLAN assignment based on the incoming packets it receives. An access port can be assigned to only one VLAN.

The **no switchport access** command resets the access mode VLAN to the appropriate default VLAN for the device.

You must configure the VMPS server (such as a Catalyst 6500 series switch) before configuring a port as dynamic.

These restrictions apply to dynamic-access ports:

- The software implements the VLAN Query Protocol (VQP) client, which can query a VMPS, such as a Catalyst 6500 series switch. The switch cannot be a VMPS. You must configure the server before configuring a port configured as dynamic.
- Use dynamic-access ports only to connect end stations. Connecting them to switches or routers (that use bridging protocols) can cause a loss of connectivity.
- Configure the network so that STP does not put the dynamic-access port into an STP blocking state. The Port Fast feature is automatically enabled on dynamic-access ports.
- Dynamic-access ports can only be in one VLAN and do not use VLAN tagging.
- Dynamic-access ports cannot be configured as
  - Members of an EtherChannel port group (dynamic-access ports cannot be grouped with any other port, including other dynamic ports).
  - Source or destination ports in a static address entry.
  - Monitor ports.

You can verify your setting by entering the **show interfaces** *vlan-id* **switchport** privileged EXEC command and examining information in the Administrative Mode and Operational Mode rows.

Examples

This example shows how to change a switched port interface that is operating in access mode to operate in VLAN 2 instead of the default VLAN:

```
Controller(config-if)# switchport access vlan 2
```

Related Commands

Command	Description
switchport mode	Configures the VLAN membership mode of a port.

switchport mode

To configure the VLAN membership mode of a port, use the **switchport mode** command in interface configuration mode. To reset the mode to the appropriate default for the device, use the **no** form of this command.

switchport mode {**access**| **dot1q-tunnel**| **dynamic** {**auto**| **desirable**}| **private-vlan**| **trunk**}

no switchport mode {**access**| **dot1q-tunnel**| **dynamic**| **trunk**}

Syntax Description

access	Sets the port to access mode (either static-access or dynamic-access depending on the setting of the **switchport access vlan** interface configuration command). The port is set to access unconditionally and operates as a nontrunking, single VLAN interface that sends and receives nonencapsulated (non-tagged) frames. An access port can be assigned to only one VLAN.
dot1q-tunnel	Sets the port as an IEEE 802.1Q tunnel port.
dynamic auto	Sets the port trunking mode dynamic parameter to auto to specify that the interface convert the link to a trunk link. This is the default switchport mode.
dynamic desirable	Sets the port trunking mode dynamic parameter to desirable to specify that the interface actively attempt to convert the link to a trunk link.
private-vlan	See the **switchport mode private-vlan** command.
trunk	Sets the port to trunk unconditionally. The port is a trunking VLAN Layer 2 interface. The port sends and receives encapsulated (tagged) frames that identify the VLAN of origination. A trunk is a point-to-point link between two controllers or between a controller and a router.

Command Default

The default mode is **dynamic auto**.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

A configuration that uses the **access**, **dot1q-tunnel**, or **trunk** keywords takes effect only when you configure the port in the appropriate mode by using the **switchport mode** command. The static-access and trunk configuration are saved, but only one configuration is active at a time.

When you enter **access** mode, the interface changes to permanent nontrunking mode and negotiates to convert the link into a nontrunk link even if the neighboring interface does not agree to the change.

When you enter **trunk** mode, the interface changes to permanent trunking mode and negotiates to convert the link into a trunk link even if the interface connecting to it does not agree to the change.

When you enter **dynamic auto** mode, the interface converts the link to a trunk link if the neighboring interface is set to **trunk** or **desirable** mode.

When you enter **dynamic desirable** mode, the interface becomes a trunk interface if the neighboring interface is set to **trunk**, **desirable**, or **auto** mode.

To autonegotiate trunking, the interfaces must be in the same VLAN Trunking Protocol (VTP) domain. Trunk negotiation is managed by the Dynamic Trunking Protocol (DTP), which is a point-to-point protocol. However, some internetworking devices might forward DTP frames improperly, which could cause misconfigurations. To avoid this, you should configure interfaces connected to devices that do not support DTP to not forward DTP frames, which turns off DTP.

- If you do not intend to trunk across those links, use the **switchport mode access** interface configuration command to disable trunking.
- To enable trunking to a device that does not support DTP, use the **switchport mode trunk** and **switchport nonegotiate** interface configuration commands to cause the interface to become a trunk but to not generate DTP frames.

When you enter **dot1q-tunnel**, the port is set unconditionally as an IEEE 802.1Q tunnel port.

Access ports, trunk ports, and tunnel ports are mutually exclusive.

Any IEEE 802.1Q encapsulated IP packets received on a tunnel port can be filtered by MAC access control lists (ACLs), but not by IP ACLs. This is because the controller does not recognize the protocol inside the IEEE 802.1Q header. This restriction applies to router ACLs, port ACLs, and VLAN maps.

Configuring a port as an IEEE 802.1Q tunnel port has these limitations:

- IP routing and fallback bridging are not supported on tunnel ports.
- Tunnel ports do not support IP ACLs.
- If an IP ACL is applied to a trunk port in a VLAN that includes tunnel ports, or if a VLAN map is applied to a VLAN that includes tunnel ports, packets received from the tunnel port are treated as non-IP packets and are filtered with MAC access lists.
- Layer 3 quality of service (QoS) ACLs and other QoS features related to Layer 3 information are not supported on tunnel ports.

For more information about configuring IEEE 802.1Q tunnel ports, see the software configuration guide for this release.

The IEEE 802.1x feature interacts with switchport modes in these ways:

- If you try to enable IEEE 802.1x on a trunk port, an error message appears, and IEEE 802.1x is not enabled. If you try to change the mode of an IEEE 802.1x-enabled port to trunk, the port mode is not changed.
- If you try to enable IEEE 802.1x on a port set to **dynamic auto** or **dynamic desirable**, an error message appears, and IEEE 802.1x is not enabled. If you try to change the mode of an IEEE 802.1x-enabled port to **dynamic auto** or **dynamic desirable**, the port mode is not changed.

- If you try to enable IEEE 802.1x on a dynamic-access (VLAN Query Protocol [VQP]) port, an error message appears, and IEEE 802.1x is not enabled. If you try to change an IEEE 802.1x-enabled port to dynamic VLAN assignment, an error message appears, and the VLAN configuration is not changed.

You can verify your settings by entering the **show interfaces** *interface-id* **switchport** privileged EXEC command and examining information in the *Administrative Mode* and *Operational Mode* rows.

Examples

This example shows how to configure a port for access mode:

```
Controller(config)# interface gigabitethernet2/0/1
Controller(config-if)# switchport mode access
```

This example shows how set the port to dynamic desirable mode:

```
Controller(config)# interface gigabitethernet2/0/1
Controller(config-if)# switchport mode dynamic desirable
```

This example shows how to configure a port for trunk mode:

```
Controller(config)# interface gigabitethernet2/0/1
Controller(config-if)# switchport mode trunk
```

This example shows how to configure a port as an IEEE 802.1Q tunnel port:

```
Controller(config)# interface gigabitethernet2/0/1
Controller(config-if)# switchport mode dot1q-tunnel
```

Related Commands

Command	Description
switchport access vlan	Configures a port as a static-access or dynamic-access port.

switchport nonegotiate

To specify that Dynamic Trunking Protocol (DTP) negotiation packets are not sent on the Layer 2 interface, use the **switchport nonegotiate** command in interface configuration mode. Use the **no** form of this command to return to the default setting.

switchport nonegotiate

no switchport nonegotiate

Syntax Description

This command has no keywords or arguments.

Command Default

The default is to use DTP negotiation to learn the trunking status.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The **no switchport nonegotiate** command removes nonegotiate status.

This command is valid only when the interface switchport mode is access or trunk (configured by using the **switchport mode access** or the **switchport mode trunk** interface configuration command). This command returns an error if you attempt to execute it in dynamic (auto or desirable) mode.

Internetworking devices that do not support DTP might forward DTP frames improperly and cause misconfigurations. To avoid this problem, turn off DTP by using the **switchport nonegotiate** command to configure the interfaces connected to devices that do not support DTP to not forward DTP frames.

When you enter the **switchport nonegotiate** command, DTP negotiation packets are not sent on the interface. The device does or does not trunk according to the **mode** parameter: **access** or **trunk.**

- If you do not intend to trunk across those links, use the **switchport mode access** interface configuration command to disable trunking.
- To enable trunking on a device that does not support DTP, use the **switchport mode trunk** and **switchport nonegotiate** interface configuration commands to cause the interface to become a trunk but to not generate DTP frames.

Examples

This example shows how to cause a port to refrain from negotiating trunking mode and to act as a trunk or access port (depending on the mode set):

```
Controller(config)# interface gigabitethernet2/0/1
Controller(config-if)# switchport nonegotiate
```

You can verify your setting by entering the **show interfaces** *interface-id* **switchport** privileged EXEC command.

Related Commands

Command	Description
switchport mode	Configures the VLAN membership mode of a port.

udld

To enable aggressive or normal mode in the UniDirectional Link Detection (UDLD) and to set the configurable message timer time, use the **udld** command in global configuration mode. To disable aggressive or normal mode UDLD on all fiber-optic ports, use the **no** form of the command.

udld {**aggressive**| **enable**| **message time** *message-timer-interval*}

no udld {**aggressive**| **enable**| **message**}

Syntax Description

aggressive	Enables UDLD in aggressive mode on all fiber-optic interfaces.
enable	Enables UDLD in normal mode on all fiber-optic interfaces.
message time *message-timer-interval*	Configures the period of time between UDLD probe messages on ports that are in the advertisement phase and are determined to be bidirectional. The range is 1 to 90 seconds. The default is 15 seconds.

Command Default

UDLD is disabled on all interfaces.

The message timer is set at 15 seconds.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

UDLD supports two modes of operation: normal (the default) and aggressive. In normal mode, UDLD detects unidirectional links due to misconnected interfaces on fiber-optic connections. In aggressive mode, UDLD also detects unidirectional links due to one-way traffic on fiber-optic and twisted-pair links and due to misconnected interfaces on fiber-optic links. For information about normal and aggressive modes, see the *Catalyst 2960-X Switch Layer 2 Configuration GuideCatalyst 2960-XR Switch Layer 2 Configuration GuideLayer 2 Configuration Guide (Cisco WLC 5700 Series)*.

If you change the message time between probe packets, you are making a trade-off between the detection speed and the CPU load. By decreasing the time, you can make the detection-response faster but increase the load on the CPU.

This command affects fiber-optic interfaces only. Use the **udld** interface configuration command to enable UDLD on other interface types.

You can use these commands to reset an interface shut down by UDLD:

- The **udld reset** privileged EXEC command to reset all interfaces shut down by UDLD.

- The **shutdown** and **no shutdown** interface configuration commands.
- The **no udld enable** global configuration command followed by the **udld {aggressive | enable}** global configuration command to reenable UDLD globally.
- The **no udld port** interface configuration command followed by the **udld port** or **udld port aggressive** interface configuration command to reenable UDLD on the specified interface.
- The **errdisable recovery cause udld** and **errdisable recovery interval** *interval* global configuration commands to automatically recover from the UDLD error-disabled state.

Examples

This example shows how to enable UDLD on all fiber-optic interfaces:

```
Controller(config)# udld enable
```

You can verify your setting by entering the **show udld** privileged EXEC command.

Related Commands

Command	Description
show udld	Displays UDLD administrative and operational status for all ports or the specified port.
udld port	Enables UDLD on an individual interface or prevents a fiber-optic interface from being enabled by the **udld** global configuration command.
udld reset	Resets all interfaces shut down by UDLD and permits traffic to pass through again.

udld port

To enable UniDirectional Link Detection (UDLD) on an individual interface or to prevent a fiber-optic interface from being enabled by the **udld** global configuration command, use the **udld port** command in interface configuration mode. To return to the **udld** global configuration command setting or to disable UDLD if entered for a nonfiber-optic port, use the **no** form of this command.

udld port [aggressive]

no udld port [aggressive]

Syntax Description

aggressive	(Optional) Enables UDLD in aggressive mode on the specified interface.

Command Default

On fiber-optic interfaces, UDLD is disabled and fiber-optic interfaces enable UDLD according to the state of the **udld enable** or **udld aggressive** global configuration command.

On nonfiber-optic interfaces, UDLD is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

A UDLD-capable port cannot detect a unidirectional link if it is connected to a UDLD-incapable port of another controller.

UDLD supports two modes of operation: normal (the default) and aggressive. In normal mode, UDLD detects unidirectional links due to misconnected interfaces on fiber-optic connections. In aggressive mode, UDLD also detects unidirectional links due to one-way traffic on fiber-optic and twisted-pair links and due to misconnected interfaces on fiber-optic links.

To enable UDLD in normal mode, use the **udld port** interface configuration command. To enable UDLD in aggressive mode, use the **udld port aggressive** interface configuration command.

Use the **no udld port** command on fiber-optic ports to return control of UDLD to the **udld enable** global configuration command or to disable UDLD on nonfiber-optic ports.

Use the **udld port aggressive** command on fiber-optic ports to override the setting of the **udld enable** or **udld aggressive** global configuration command. Use the **no** form on fiber-optic ports to remove this setting and to return control of UDLD enabling to the **udld** global configuration command or to disable UDLD on nonfiber-optic ports.

You can use these commands to reset an interface shut down by UDLD:

- The **udld reset** privileged EXEC command resets all interfaces shut down by UDLD.

- The **shutdown** and **no shutdown** interface configuration commands.
- The **no udld enable** global configuration command, followed by the **udld {aggressive | enable}** global configuration command reenables UDLD globally.
- The **no udld port** interface configuration command, followed by the **udld port** or **udld port aggressive** interface configuration command reenables UDLD on the specified interface.
- The **errdisable recovery cause udld** and **errdisable recovery interval** *interval* global configuration commands automatically recover from the UDLD error-disabled state.

Examples

This example shows how to enable UDLD on an port:

```
Controller(config)# interface gigabitethernet6/0/1
Controller(config-if)# udld port
```

This example shows how to disable UDLD on a fiber-optic interface despite the setting of the **udld** global configuration command:

```
Controller(config)# interface gigabitethernet6/0/1
Controller(config-if)# no udld port
```

You can verify your settings by entering the **show running-config** or the **show udld** *interface* privileged EXEC command.

Related Commands

Command	Description
show udld	Displays UDLD administrative and operational status for all ports or the specified port.
udld	Enables aggressive or normal mode in UDLD or sets the configurable message timer time.
udld reset	Resets all interfaces shut down by UDLD and permits traffic to pass through again.

udld reset

To reset all interfaces disabled by UniDirectional Link Detection (UDLD) and permit traffic to begin passing through them again (though other features, such as spanning tree, Port Aggregation Protocol (PAgP), and Dynamic Trunking Protocol (DTP) still have their normal effects, if enabled), use the **udld reset** command in privileged EXEC mode.

udld reset

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

If the interface configuration is still enabled for UDLD, these ports begin to run UDLD again and are disabled for the same reason if the problem has not been corrected.

Examples

This example shows how to reset all interfaces disabled by UDLD:

```
Controller# udld reset
1 ports shutdown by UDLD were reset.
```

Related Commands

Command	Description
show udld	Displays UDLD administrative and operational status for all ports or the specified port.
udld	Enables aggressive or normal mode in UDLD or sets the configurable message timer time.
udld port	Enables UDLD on an individual interface or prevents a fiber-optic interface from being enabled by the **udld** global configuration command.

PART IX

WLAN

WLAN Commands

aaa-override

To enable AAA override on the WLAN, use the **aaa-override** command. To disable AAA override, use the **no** form of this command.

aaa-override

no aaa-override

Syntax Description

This command has no keywords or arguments.

Command Default

AAA is disabled by default.

Command Modes

wlan

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You must disable the WLAN before using this command.

Examples

This example shows how to enable AAA on a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)# shutdown
Controller(config)# wlan wlan1
Controller(config-wlan)# aaa-override
Controller(config)# no shutdown
Controller(config-wlan)# end
```

This example shows how to disable AAA on a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)# shutdown
Controller(config)# wlan wlan1
Controller(config-wlan)# no aaa-override
Controller(config)# no shutdown
Controller(config-wlan)# end
```

accounting-list

To configure RADIUS accounting servers on a WLAN, use the **accounting-list** command. To disable RADIUS server accounting, use the **no** form of this command.

accounting-list *radius-server-acct*

no accounting-list

Syntax Description

radius-server-acct	Accounting RADIUS server name.

Command Default

RADIUS server accounting is disabled by default.

Command Modes

wlan

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You must disable the WLAN before using this command.

Examples

This example shows how to configure RADIUS server accounting on a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# accounting-list test
Controller(config-wlan)# end
```

This example shows how to disable RADIUS server accounting on a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# no accounting-list test
Controller(config-wlan)# end
```

band-select

To configure band selection on a WLAN, use the **band-select** command. To disable band selection, use the **no** form of this command.

band-select

no band-select

Syntax Description

This command has no keywords or arguments.

Command Default

Band selection is disabled by default.

Command Modes

wlan

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

When you enable band select on a WLAN, the access point suppresses client probes on 2.4GHz and moves the dual band clients to the 5-GHz spectrum. The band-selection algorithm directs dual-band clients only from the 2.4-GHz radio to the 5-GHz radio of the same access point, and it only runs on an access point when both the 2.4-GHz and 5-GHz radios are up and running.

You must disable the WLAN before using this command.

Examples

This example shows how to enable band select on a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# band-select
Controller(config-wlan)# end
```

This example shows how to disable band selection on a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# no band-select
Controller(config-wlan)# end
```

broadcast-ssid

To enable a Service Set Identifier (SSID) on a WLAN, use the **broadcast-ssid** command. To disable broadcasting of SSID, use the **no** form of this command.

broadcast-ssid

no broadcast-ssid

Syntax Description

This command has no keywords or arguments.

Command Default

The SSIDs of WLANs are broadcasted by default.

Command Modes

wlan

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You must disable the WLAN before using this command.

Examples

This example shows how to enable a broadcast SSID on a WLAN.

```
Controller# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# broadcast-ssid
Controller(config-wlan)# end
```

This example shows how to disable a broadcast SSID on a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# no broadcast-ssid
Controller(config-wlan)# end
```

call-snoop

To enable Voice over IP (VoIP) snooping on a WLAN, use the **call-snoop** command. To disable Voice over IP (VoIP), use the **no** form of this command.

call-snoop

no call-snoop

Syntax Description

This command has no keywords or arguments.

Command Default

VoIP snooping is disabled by default.

Command Modes

wlan

Usage Guidelines

You must disable the WLAN before using this command.

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The WLAN on which call snooping is configured must be configured with Platinum QoS. You must disable quality of service before using this command.

Examples

This example shows how to enable VoIP on a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# call-snoop
Controller(config-wlan)# end
```

This example shows how to disable VoIP on a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# no call-snoop
Controller(config-wlan)# end
```

channel-scan defer-priority

To configure the device to defer priority markings for packets that can defer off-channel scanning, use the **channel-scan defer-priority** command. To disable the device to defer priority markings for packets that can defer off-channel scanning, use the **no** form of this command.

channel-scan defer-priority *priority*

no channel-scan defer-priority *priority*

Syntax Description

priority	Channel priority value. The range is 0 to 7. The default is 3.

Command Default

Channel scan defer is enabled.

Command Modes

wlan

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to enable channel scan defer priority on a WLAN and set it to a priority value 4:

```
Controller# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# channel-scan defer-priority 4
Controller(config-wlan)# end
```

This example shows how to disable channel scan defer priority on a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# no channel-scan defer-priority 4
Controller(config-wlan)# end
```

channel-scan defer-time

To assign a channel scan defer time, use the **channel-scan defer-time** command. To disable the channel scan defer time, use the **no** form of this command.

channel-scan defer-time *msecs*

no channel-scan defer-time

Syntax Description

msecs	Deferral time in milliseconds. The range is from 0 to 60000. The default is 100.

Command Default

Channel-scan defer time is enabled.

Command Modes

wlan

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The time value in milliseconds should match the requirements of the equipment on the WLAN.

Examples

This example shows how to enable a channel scan on the WLAN and set the scan deferral time to 300 milliseconds:

```
Controller# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# channel-scan defer-time 300
Controller(config-wlan)# end
```

This example shows how to disable channel scan defer time on a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# no channel-scan defer-time
Controller(config-wlan)# end
```

chd

To enable coverage hole detection on a WLAN, use the **chd** command. To disable coverage hole detection, use the **no** form of this command.

chd

no chd

Syntax Description

This command has no keywords or arguments.

Command Default

Coverage hole detection is enabled.

Command Modes

wlan

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Examples

This example shows how to enable coverage hole detection on a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# chd
Controller(config-wlan)# end
```

This example shows how to disable coverage hole detection on a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# no chd
Controller(config-wlan)# end
```

client association limit

To configure the maximum number of client connections on a WLAN, use the **client association limit** command. To disable clients on the WLAN, use the **no** form of this command.

client association limit *max-clients*

no client association limit

Syntax Description

max-clients	Number of client connections to be accepted. The range is from 0 to 12000. A value of zero (0) indicates no set limit.

Command Default

The max-client value is set to 0 (no limit).

Command Modes

wlan

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You must disable the WLAN before using this command.

Examples

This example shows how to configure a client association limit on a WLAN and configure the client limit to 200:

```
Controller# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# client association limit 200
Controller(config-wlan)# end
```

This example shows how to disable a client association limit on a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# no client association limit
Controller(config-wlan)# end
```

client vlan

To configure a WLAN interface or an interface group, use the **client vlan** command. To disable the WLAN interface, use the **no** form of this command.

client vlan *interface-id-name-or-group-name*

no client vlan

Syntax Description

interface--id-name-or-group-name	Interface ID, name, or VLAN group name.

Command Default

The default interface is configured.

Command Modes

wlan

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You must disable the WLAN before using this command.

Examples

This example shows how to enable a client VLAN on a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# client vlan client-vlan1
Controller(config-wlan)# end
```

This example shows how to disable a client association limit on a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# no client vlan
Controller(config-wlan)# end
```

ccx aironet-iesupport

To enable Aironet Information Elements (IEs) for a WLAN, use the **ccx aironet-iesupport** command. To disable Aironet Information Elements (IEs), use the **no** form of this command.

ccx aironet-iesupport

no ccx aironet-iesupport

Syntax Description

This command has no keywords or arguments.

Command Default

Aironet IE support is enabled.

Command Modes

wlan

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You must disable the WLAN before using this command.

Examples

This example shows how to enable an Aironet IE for a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# ccx aironet-iesupport
Controller(config-wlan)# end
```

This example shows how to disable an Aironet IE on a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# no ccx aironet-iesupport
Controller(config-wlan)# end
```

datalink flow monitor

To enable NetFlow monitoring in a WLAN, use the **datalink flow monitor** command. To disable NetFlow monitoring, use the **no** form of this command.

datalink flow monitor *datalink-monitor-name* {**input| output**}

no datalink flow monitor *datalink-monitor-name* {**input| output**}

Syntax Description

datalink-monitor-name	Flow monitor name.
input	Specifies the NetFlow monitor for ingress traffic.
output	Specifies the NetFlow monitor for egress traffic.

Command Default

Command Modes

wlan

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You must disable the WLAN before using this command.

Examples

This example shows how to enable NetFlow monitoring on a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# datalink flow monitor test output
Controller(config-wlan)# end
```

This example shows how to disable NetFlow monitoring on a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# no datalink flow monitor test output
Controller(config-wlan)# end
```

default

default {**aaa-override**| **accounting-list**| **band-select**| **broadcast-ssid**| **call-snoop**| **ccx**| **channel-scan**| **parameters**| **chd**| **client**| **datalink**| **diag-channel**| **dtim**| **exclusionlist**| **ip**| **ipv6**| **load-balance**| **local-auth**| **mac-filtering**| **media-stream**| **mfp**| **mobility**| **nac**| **passive-client**| **peer-blocking**| **radio**| **roamed-voice-client**| **security**| **service-policy**| **session-timeout**| **shutdown**| **sip-cac**| **static-ip**| **uapsd**| **wgb**| **wmm**}

Syntax Description

aaa-override	Sets the AAA override parameter to its default value.
accounting-list	Sets the accounting parameter and its attributes to their default values.
band-select	Sets the band selection parameter to its default values.
broadcast-ssid	Sets the broadcast Service Set Identifier (SSID) parameter to its default value.
call-snoop	Sets the call snoop parameter to its default value.
ccx	Sets the Cisco client extension (Cisco Aironet IE) parameters and attributes to their default values.
channel-scan	Sets the channel scan parameters and attributes to their default values.
chd	Sets the coverage hold detection parameter to its default value.
client	Sets the client parameters and attributes to their default values.
datalink	Sets the datalink parameters and attributes to their default values.
diag-channel	Sets the diagnostic channel parameters and attributes to their default values.
dtim	Sets the Delivery Traffic Indicator Message (DTIM) parameter to its default value.
exclusionlist	Sets the client exclusion timeout parameter to its default value.
ip	Sets the IP parameters to their default values.
ipv6	Sets the IPv6 parameters and attributes to their default values.
load-balance	Sets the load-balancing parameter to its default value.
local-auth	Sets the Extensible Authentication Protocol (EAP) profile parameters and attributes to their default values.
mac-filtering	Sets the MAC filtering parameters and attributes to their default values.
media-stream	Sets the media stream parameters and attributes to their default values.

mfp	Sets the Management Frame Protection (MPF) parameters and attributes to their default values.
mobility	Sets the mobility parameters and attributes to their default values.
nac	Sets the RADIUS Network Admission Control (NAC) parameter to its default value.
passive-client	Sets the passive client parameter to its default value.
peer-blocking	Sets the peer to peer blocking parameters and attributes to their default values.
radio	Sets the radio policy parameters and attributes to their default values.
roamed-voice-client	Sets the roamed voice client parameters and attributes to their default values.
security	Sets the security policy parameters and attributes to their default values.
service-policy	Sets the WLAN quality of service (QoS) policy parameters and attributes to their default values.
session-timeout	Sets the client session timeout parameter to its default value.
shutdown	Sets the shutdown parameter to its default value.
sip-cac	Sets the Session Initiation Protocol (SIP) Call Admission Control (CAC) parameters and attributes to their default values.
static-ip	Sets the static IP client tunneling parameters and their attributes to their default values.
uapsd	Sets the Wi-Fi Multimedia (WMM) Unscheduled Automatic Power Save Delivery (UAPSD) parameters and attributes to their default values.
wgb	Sets the Workgroup Bridges (WGB) parameter to its default value.
wmm	Sets the WMM parameters and attributes to their default values.

Command Default

None.

Command Modes

wlan

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines You must disable the WLAN before using this command.

Examples This example shows how to set the Cisco Client Extension parameter to its default value:

```
Controller(config-wlan)# default ccx aironet-iesupport
```

dtim dot11

To configure the Delivery Traffic Indicator Message (DTIM) period for a WLAN, use the **dtim dot11** command. To disable DTIM, use the **no** form of this command.

dtim dot11 {**5ghz**| **24ghz**} *dtim-period*

no dtim dot11 {**5ghz**| **24ghz**} *dtim-period*

Syntax Description

5ghz	Configures the DTIM period on the 5-GHz band.
24ghz	Configures the DTIM period on the 2.4-GHz band.
dtim-period	Value for the DTIM period. The range is from 1 to 255.

Command Default

The DTIM period is set to 1.

Command Modes

wlan

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You must disable the WLAN before using this command.

Examples

This example shows how to enable the DTIM period on a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# dtim dot11 24ghz 3
```

This example shows how to disable the DTIM period on a WLAN on the 2.4-GHz band:

```
Controller# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# no dtim dot11 24ghz 3
```

exclusionlist

To configure an exclusion list on a wireless LAN, use the **exclusionlist** command. To disable an exclusion list, use the **no** form of this command.

exclusionlist [**timeout** *seconds*]

no exclusionlist [timeout]

Syntax Description

timeout *seconds*	(Optional) Specifies an exclusion list timeout in seconds. The range is from 0 to 2147483647. A value of zero (0) specifies no timeout.

Command Default

The exclusion list is set to 60 seconds.

Command Modes

wlan

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You must disable the WLAN before using this command.

Examples

This example shows how to configure a client exclusion list for a WLAN:

```
Controller#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)#wlan wlan1
Controller(config-wlan)#exclusionlist timeout 345
```

This example shows how to disable a client exclusion list on a WLAN:

```
Controller#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)#wlan wlan1
Controller(config-wlan)#no exclusionlist timeout 345
```

exit

To exit the WLAN configuration submode, use the **exit** command.

exit

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

wlan

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to exit the WLAN configuration submode:

```
Controller# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# exit
Controller(config)#
```

exit (WLAN AP Group)

To exit the WLAN AP group submode, use the **exit** command.

exit

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

wlan-apgroup

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to exit the WLAN AP group submode:

```
Controller# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)# ap group test
Controller(config-apgroup)# exit
```

ip access-group

To configure WLAN access control group (ACL), use the **ip access-group** command. To remove a WLAN ACL group, use the **no** form of the command.

ip access-group [web] *acl-name*

no ip access-group [web]

Syntax Description

web	(Optional) Configures the IPv4 web ACL.
acl-name	IPv4 ACL name.

Command Default

None

Command Modes

wlan

Usage Guidelines

You must disable the WLAN before using this command.

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to configure a WLAN ACL:

```
Controller#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)#wlan wlan1
Controller(config-wlan)#ip access-group test-acl
```

This example shows how to configure an IPv4 WLAN web ACL:

```
Controller# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# ip access-group web test
Controller(config-wlan)#
```

ip flow monitor

To configure IP NetFlow monitoring, use the **ip flow monitor** command. To remove IP NetFlow monitoring, use the **no** form of this command.

ip flow monitor *ip-monitor-name* {**input**| **output**}

no ip flow monitor *ip-monitor-name* {**input**| **output**}

Syntax Description

ip-monitor-name	Flow monitor name.
input	Enables a flow monitor for ingress traffic.
output	Enables a flow monitor for egress traffic.

Command Default

None

Command Modes

wlan

Usage Guidelines

You must disable the WLAN before using this command.

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to configure an IP flow monitor for the ingress traffic:

```
Controller# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# ip flow monitor test input
```

This example shows how to disable an IP flow monitor:

```
Controller# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# no ip flow monitor test input
```

ip verify source mac-check

To enable IPv4 Source Guard (IPSG) on a WLAN, use the **ip verify source mac-check** command. To disable IPSG, use the **no** form of this command.

ip verify source mac-check

no ip verify source mac-check

Syntax Description

This command has no keywords or arguments.

Command Default

IPSG is disabled.

Command Modes

wlan

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Use this feature to restrict traffic from a host to a specific interface that is based on the host's IP address. The feature can also be configured to bind the source MAC and IP of a host so that IP spoofing is prevented.

Use this feature to bind the IP and MAC address of a wireless host that is based on information received from DHCP snooping, ARP, and Dataglean. Dataglean is the process of extracting location information such as host hardware address, ports that lead to the host, and so on from DHCP messages as they are forwarded by the DHCP relay agent. If a wireless host tries to send traffic with IP address and MAC address combination that has not been learned by the controller, this traffic is dropped in the hardware. IPSG is not supported on DHCP packets. IPSG is not supported for foreign clients in a foreign controller.

You must disable the WLAN before using this command.

Examples

This example shows how to enable IPSG:

```
Controller# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# ip verify source mac-check
```

This example shows how to disable IPSG:

```
Controller# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# no ip verify source mac-check
```

load-balance

To enable load balancing on a WLAN, use the **load-balance** command. To disable load balancing, use the **no** form of this command.

load-balance

no load-balance

Syntax Description

This command has no keywords or arguments.

Command Default

Load balancing is disabled by default.

Command Modes

wlan

Command History

Release	Modification
Cisco IOS XE 3.2SE	The command was introduced.

Usage Guidelines

You must disable the WLAN before using this command.

Examples

This example shows how to enable load balancing on a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)# shutdown
Controller(config)# wlan wlan1
Controller(config-wlan)# load-balance
Controller(config)# no shutdown
Controller(config-wlan)# end
```

This example shows how to disable load balancing on a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)# shutdown
Controller(config)# wlan wlan1
Controller(config-wlan)# no load-balance
Controller(config)# no shutdown
Controller(config-wlan)# end
```

nac

To enable RADIUS Network Admission Control (NAC) support for a WLAN, use the **nac** command. To disable NAC out-of-band support, use the **no** form of this command.

nac

no nac

Syntax Description

This command has no keywords or arguments.

Command Default

NAC is disabled.

Command Modes

wlan

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You should enable AAA override before you enable the RADIUS NAC state.

Examples

This example shows how to configure RADIUS NAC on the WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# aaa-override
Controller(config-wlan)# nac
```

This example shows how to disable RADIUS NAC on the WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# no nac
Controller(config-wlan)# no aaa-override
```

Related Commands

Command	Description
aaa-override	Enables or disables AAA override on a WLAN.

passive-client

To enable the passive client feature on a WLAN, use the **passive-client** command. To disable the passive client feature, use the **no** form of this command.

passive-client

no passive-client

Syntax Description

This command has no keywords or arguments.

Command Default

Passive client feature is disabled.

Command Modes

wlan

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You must enable the global multicast mode and multicast-multicast mode before entering this command. Both multicast-multicast mode and multicast unicast modes are supported. The multicast-multicast mode is recommended.

You must disable the WLAN before using this command.

Examples

This show how to enable the passive client feature on a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)# wireless multicast
Controller(config)# wlan test-wlan
Controller(config-wlan)# passive-client
```

This example shows how to disable the passive client feature on a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)# wireless multicast
Controller(config)# wlan test-wlan
Controller(config-wlan)# no passive-client
```

peer-blocking

To configure peer-to-peer blocking on a WLAN, use the **peer-blocking** command. To disable peer-to-peer blocking, use the **no** form of this command.

peer-blocking {**drop**| **forward-upstream**}

no peer-blocking

Syntax Description

drop	Specifies the controller to discard the packets.
forward-upstream	Specifies the packets to be forwarded on the upstream VLAN. The device next in the hierarchy to the controller decides what action to take regarding the packets.

Command Default

Peer blocking is disabled.

Command Modes

wlan

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You must disable the WLAN before using this command.

Examples

This example shows how to enable the drop and forward-upstream options for peer-to-peer blocking:

```
Controller# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# peer-blocking  drop
Controller(config-wlan)# peer-blocking forward-upstream
```

This example shows how to disable the drop and forward-upstream options for peer-to-peer blocking:

```
Controller# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# no peer-blocking  drop
Controller(config-wlan)# no peer-blocking forward-upstream
```

radio

To enable the Cisco radio policy on a WLAN, use the **radio** command. To disable the Cisco radio policy on a WLAN, use the **no** form of this command.

radio {**all**| **dot11a**| **dot11ag**| **dot11bg**| **dot11g**}

no radio

Syntax Description

all	Configures the WLAN on all radio bands.
dot11a	Configures the WLAN on only 802.11a radio bands.
dot11ag	Configures the WLAN on 802.11a/g radio bands.
dot11bg	Configures the wireless LAN on only 802.11b/g radio bands (only 802.11b if 802.11g is disabled).
dot11g	Configures the wireless LAN on 802.11g radio bands only.

Command Default

Radio policy is enabled on all bands.

Command Modes

wlan

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You must disable the WLAN before using this command.

Examples

This example shows how to configure the WLAN on all radio bands:

```
Controller# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# radio all
```

This example shows how to disable all radio bands on a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# no radio all
```

radio-policy

To configure the radio policy on a WLAN AP group, use the **radio** command. To disable the radio policy on the WLAN, use the **no** form of this command.

radio-policy {**all**| **dot11a**| **dot11bg**| **dot11g**}

no radioall| **dot11a**| **dot11bg**| **dot11g**

Syntax Description

all	Configures the wireless LAN on all radio bands.
dot11a	Configures the wireless LAN on only 802.11a radio bands.
dot11bg	Configures the wireless LAN on only 802.11b/g (only 802.11b if 802.11g is disabled) radio bands.
dot11g	Configures the wireless LAN on only 802.11g radio bands.

Command Default

Radio policy is enabled on all the bands.

Command Modes

wlan-apgroup

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The WLAN must be restarted for the changes to take effect.

Examples

This example shows how to enable the radio policy on the 802.11b band for an AP group:

```
Controller(config)# ap group test
Controller(config-apgroup)# wlan test-wlan
Controller(config-wlan-apgroup)# radio-policy dot11b
```

This example shows how to disable the radio policy on the 802.11b band of an AP group:

```
Controller(config)# ap group test
Controller(config-apgroup)# wlan test-wlan
Controller(config-wlan-apgroup)# no radio-policy dot11bg
```

roamed-voice-client re-anchor

To enable the roamed-voice-client re-anchor feature, use the **roamed-voice-client re-anchor** command. To disable the roamed-voice-client re-anchor feature, use the **no** form of this command.

roamed-voice-client re-anchor

no roamed-voice-client re-anchor

Syntax Description

This command has no keywords or arguments.

Command Default

Roamed voice client reanchor feature is disabled.

Command Modes

wlan

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You must disable the WLAN before using this command.

Examples

This example shows how to enable the roamed voice client re-anchor feature:

```
Controller# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# roamed-voice-client re-anchor
```

This example shows how to disable the roamed voice client re-anchor feature:

```
Controller# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# no roamed-voice-client re-anchor
```

session-timeout

To configure session timeout for clients associated to a WLAN, use the **session-timeout** command. To disable a session timeout for clients that are associated to a WLAN, use the **no** form of this command.

session-timeout seconds

no session-timeout

Syntax Description

seconds	Timeout or session duration in seconds. A value of zero (0) is equivalent to no timeout. The range is from 300 to 86400.

Command Default

The client timeout is set to 1800 seconds for WLANs that are configured with dot1x security. The client timeout is set to 0 for open WLANs.

Command Modes

wlan

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to configure a session timeout to 300 seconds:

```
Controller# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# session-timeout 300
```

This example shows how to disable a session timeout:

```
Controller# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# no session-timeout
```

service-policy (WLAN)

To configure the WLAN quality of service (QoS) service policy, use the **service-policy** command. To disable a QoS policy on a WLAN, use the **no** form of this command.

service-policy [client] {**input**| **output**} *policy-name*

no service-policy [client] {**input**| **output**} *policy-name*

Syntax Description

client	(Optional) Assigns a policy map to all clients in the WLAN.
input	Assigns an input policy map.
output	Assigns an output policy map.
policy-name	Policy name.

Command Default

No policies are assigned and the state assigned to the policy is None.

Command Modes

wlan

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You must disable the WLAN before using this command.

Examples

This example shows how to configure the input QoS service policy on a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# service-policy input policy-test
```

This example shows how to disable the input QoS service policy on a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# no service-policy input policy-test
```

show wlan

To view WLAN parameters, use the **show wlan** command.

show wlan {**all** | **id** *wlan-id*| **name** *wlan-name* | **summary**}

Syntax Description

all	Displays a summary of parameters of all configured WLANs. The list is ordered by the ascending order of the WLAN IDs.
id	Wireless LAN identifier. The range is from 1 to 512.
wlan-id	ID of the WLAN. The range is from 1 to 512.
name	WLAN profile name. The name is from 1 to 32 characters.
wlan-name	WLAN profile name. The name is from 1 to 32 characters.
summary	Displays a summary of the parameters configured on a WLAN.

Command Default

None.

Command Modes

Global Configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to display a summary of the WLANs configured on the device:

```
Controller# show wlan summary
Number of WLANs: 1

WLAN Profile Name                    SSID                           VLAN Status
-------------------------------------------------------------------------------
45   test-wlan                       test-wlan-ssid                  1    UP
```

This example shows how to display a summary of parameters configured on a particular WLAN:

```
Controller# show wlan test-wlan
WLAN Identifier                                 : 45
Profile Name                                    : test-wlan
Network Name (SSID)                             : test-wlan-ssid
Status                                          : Enabled
Broadcast SSID                                  : Enabled
Maximum number of Associated Clients            : 0
AAA Policy Override                             : Disabled
Network Admission Control
  NAC-State                                     : Disabled
Number of Active Clients                        : 0
Exclusionlist Timeout                           : 60
Session Timeout                                 : 1800 seconds
CHD per WLAN                                    : Enabled
Webauth DHCP exclusion                          : Disabled
Interface                                       : default
Interface Status                                : Up
Multicast Interface                             : test
WLAN IPv4 ACL                                   : test
WLAN IPv6 ACL                                   : unconfigured
DHCP Server                                     : Default
DHCP Address Assignment Required                : Disabled
DHCP Option 82                                  : Disabled
DHCP Option 82 Format                           : ap-mac
DHCP Option 82 Ascii Mode                       : Disabled
DHCP Option 82 Rid Mode                         : Disabled
QoS Service Policy - Input
  Policy Name                                   : unknown
  Policy State                                  : None
QoS Service Policy - Output
  Policy Name                                   : unknown
  Policy State                                  : None
QoS Client Service Policy
  Input  Policy Name                            : unknown
  Output Policy Name                            : unknown
WMM                                             : Disabled
Channel Scan Defer Priority:
  Priority (default)                            : 4
  Priority (default)                            : 5
  Priority (default)                            : 6
Scan Defer Time (msecs)                         : 100
Media Stream Multicast-direct                   : Disabled
CCX - AironetIe Support                         : Enabled
CCX - Gratuitous ProbeResponse (GPR)            : Disabled
CCX - Diagnostics Channel Capability            : Disabled
Dot11-Phone Mode (7920)                         : Invalid
Wired Protocol                                  : None
Peer-to-Peer Blocking Action                    : Disabled
Radio Policy                                    : All
DTIM period for 802.11a radio                   : 1
DTIM period for 802.11b radio                   : 1
Local EAP Authentication                        : Disabled
Mac Filter Authorization list name              : Disabled
Accounting list name                            : Disabled
802.1x authentication list name                 : Disabled
Security
    802.11 Authentication                       : Open System
    Static WEP Keys                             : Disabled
    802.1X                                      : Disabled
    Wi-Fi Protected Access (WPA/WPA2)           : Enabled
        WPA (SSN IE)                            : Disabled
        WPA2 (RSN IE)                           : Enabled
            TKIP Cipher                         : Disabled
            AES Cipher                          : Enabled
        Auth Key Management
            802.1x                              : Enabled
            PSK                                 : Disabled
            CCKM                                : Disabled
    IP Security                                 : Disabled
    IP Security Passthru                        : Disabled
    L2TP                                        : Disabled
```

```
    Web Based Authentication                   : Disabled
    Conditional Web Redirect                   : Disabled
    Splash-Page Web Redirect                   : Disabled
    Auto Anchor                                : Disabled
    Sticky Anchoring                           : Enabled
    Cranite Passthru                           : Disabled
    Fortress Passthru                          : Disabled
    PPTP                                       : Disabled
    Infrastructure MFP protection              : Enabled
    Client MFP                                 : Optional
    Webauth On-mac-filter Failure              : Disabled
    Webauth Authentication List Name           : Disabled
    Webauth Parameter Map                      : Disabled
    Tkip MIC Countermeasure Hold-down Timer    : 60
Call Snooping                                  : Disabled
Passive Client                                 : Disabled
Non Cisco WGB                                  : Disabled
Band Select                                    : Disabled
Load Balancing                                 : Disabled
IP Source Guard                                : Disabled
Netflow Monitor                                : test
        Direction                              : Input
        Traffic                                : Datalink

Mobility Anchor List
IP Address
-----------
```

shutdown

To disable a WLAN, use the **shutdown** command. To enable a WLAN, use the **no** form of this command.

shutdown

no shutdown

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

wlan

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to disable a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)# wlan test-wlan
Controller(config-wlan)# shutdown
Controller(config-wlan)# end
Controller# show wlan summary
Number of WLANs: 1

WLAN Profile Name                     SSID                              VLAN Status
-------------------------------------------------------------------------------------
45   test-wlan                         test-wlan-ssid                     1    DOWN
```

This example shows how to enable a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)# wlan test-wlan
Controller(config-wlan)# no shutdown
Controller(config-wlan)# end
Controller# show wlan summary
Number of WLANs: 1

WLAN Profile Name                     SSID                              VLAN Status
-------------------------------------------------------------------------------------
45   test-wlan                         test-wlan-ssid                     1    UP
```

sip-cac

To configure the Session Initiation Protocol (SIP) Call Admission Control (CAC) features on a WLAN, use the **sip-cac** command. To disable the SIP CAC feature, use the **no** form of this command.

sip-cac {**disassoc-client**| **send-486busy**}

no sip-cac {**disassoc-client**| **send-486busy**}

Syntax Description

disassoc-client	Enables a client disassociation if a CAC failure occurs.
send-486busy	Sends a SIP 486 busy message if a CAC failure occurs.

Command Default

None

Command Modes

wlan

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You must disable the WLAN before using this command.

Examples

This example shows how to enable a client disassociation and 486 busy message on a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# sip-cac disassoc-client
Controller(config-wlan)# sip-cac send-486busy
```

This example shows how to disable a client association and 486 busy message on a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# no sip-cac disassoc-client
Controller(config-wlan)# no sip-cac send-486busy
```

static-ip tunneling

To enable static IP tunneling on a WLAN, use the **static-ip tunneling** command. To disable the static IP tunneling feature, use the **no** form of this command.

static-ip tunneling

no static-ip tunneling

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

wlan

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to enable static-IP tunneling:

```
Controller# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# static-ip tunneling
```

This example shows how to disable static-IP tunneling:

```
Controller# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# no static-ip tunneling
```

vlan

To assign a VLAN to an AP group, use the **vlan** command. To remove a VLAN ID, use the **no** form of this command.

vlan *interface-name*

no vlan

Syntax Description

interface-name	VLAN interface name.

Command Default

None

Command Modes

wlan-apgroup

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You must disable the WLAN before using this command.

Examples

This example shows how to configure a VLAN on an AP group:

```
Controller# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)# ap group ap-group-1
Controller(config-apgroup)# wlan test-wlan
Controller(config-wlan-apgroup)# vlan 3
```

wgb non-cisco

To enable non-Cisco Workgroup Bridges (WGB) clients on the WLAN, use the **wgb non-cisco** command. To disable support for non-Cisco WGB clients, use the **no** form of this command.

wgb non-cisco

no wgb non-cisco

Syntax Description

This command has no keywords or arguments.

Command Default

Non-Cisco WGB clients are disabled.

Command Modes

WLAN

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You must disable the WLAN before using this command.

Examples

This example shows how to enable non-Cisco WGBs on a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# shutdown
Controller(config-wlan)# wgb non-cisco
Controller(config-wlan)# no shutdown
```

This example shows how to disable support for non-Cisco WGB clients on a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# shutdown
Controller(config-wlan)# no wgb non-cisco
Controller(config-wlan)# no shutdown
```

wlan

To configure WLAN parameters of a WLAN in an access point (AP) group, use the **wlan** command. To remove a WLAN from the AP group, use the **no** form of this command.

wlan *wlan-name*

no wlan *wlan-name*

Syntax Description

wlan-name	WLAN profile name. The range is from 1 to 32 alphanumeric characters.

Command Default

None

Command Modes

apgroup

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You must disable the WLAN before using this command.

Examples

This example shows how to enter the wlan mode in the AP group configuration mode:

```
Controller# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)# ap group test
Controller(config-apgroup)# wlan qos-wlan
```

wlan (Global Configuration Mode)

To create a wireless LAN, use the **wlan** command. To disable a wireless LAN, use the **no** form of this command.

wlan [*wlan-name*| *wlan-name wlan-id*| *wlan-name wlan-id wlan-ssid*]

no wlan [*wlan-name*| *wlan-name wlan-id*| *wlan-name wlan-id wlan-ssid*]

Syntax Description

wlan-name	WLAN profile name. The name is from 1 to 32 alphanumeric characters.
wlan-id	Wireless LAN identifier. The range is from 1 to 512.
wlan-ssid	SSID. The range is from 1 to 32 alphanumeric characters.

Command Default

WLAN is disabled.

Command Modes

Global configuration.

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

If you do not specify an SSID, the profile name parameter is used for both the profile name and the SSID. If the management and AP-manager interfaces are mapped to the same port and are members of the same VLAN, you must disable the WLAN before making a port-mapping change to either interface. If the management and AP-manager interfaces are assigned to different VLANs, you do not need to disable the WLAN.

An error message appears if you try to delete a WLAN that is assigned to an access point group. If you proceed, the WLAN is removed from the access point group and from the access point's radio.

Examples

This example shows how to create a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config)# wlan test-wlan-cr 67 test-wlan-cr-ssid
```

This example shows how to delete a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config)# no wlan test-wlan-cr 67 test-wlan-cr-ssid
```

wlan shutdown

To disable a WLAN, use the **wlan shutdown** command. To enable a WLAN, use the **no** form of this command.

wlan shutdown

no wlan shutdown

Command Default

The WLAN is disabled.

Command Modes

Global Configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You must disable the WLAN before using this command.

Examples

This example shows how to shut down a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# shutdown
```

wmm

To enable Wi-Fi Multimedia (WMM) on a WLAN, use the **wmm** command. To disable WMM on a WLAN, use the **no** form of this command.

wmm {**allowed**| **require**}

no wmm

Syntax Description

allowed	Allows WMM on a WLAN
require	Mandates that clients use WMM on the WLAN.

Command Default

WMM is enabled.

Command Modes

wlan

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

When the controller is in Layer 2 mode and WMM is enabled, you must put the access points on a trunk port in order to allow them to join the controller.

You must disable the WLAN before using this command.

Examples

This example shows how to enable WMM on a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# wmm allowed
```

This example shows how to disable WMM on a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# no wmm
```

PART X

Radio Resource Management

Radio Resource Management Commands

ap dot11 rrm

To configure basic and advanced radio resource management settings for 802.11 devices, use the **ap dot11 rrm** command.

ap dot11 {**24ghz**| **5ghz**} **rrm** {**ccx location-measurement** *sec*| **channel** {**cleanair-event**| **dca**| **device**| **foreign**| **load**| **noise**| **outdoor-ap-dca**}| **coverage** {**data fail-percentage** *pct*| **data packet-count** *count*| **data rssi-threshold** *threshold*}| **exception global** *percentage*| **level global** *number*| **voice** {**fail-percentage** *percentage*| **packet-count** *number*| **rssi-threshold** *threshold*}}

Syntax Description

ccx	Configures Advanced (RRM) 802.11 CCX options.
location-measurement	Specifies 802.11 CCX Client Location Measurements in seconds. The range is between 10 and 32400 seconds.
channel	Configure advanced 802.11-channel assignment parameters.
cleanair-event	Configures cleanair event-driven RRM parameters.
dca	Configures 802.11-dynamic channel assignment algorithm parameters.
device	Configures persistent non-WiFi device avoidance in the 802.11-channel assignment.
foreign	Enables foreign AP 802.11-interference avoidance in the channel assignment.
load	Enables Cisco AP 802.11-load avoidance in the channel assignment.
noise	Enables non-802.11-noise avoidance in the channel assignment.
outdoor-ap-dca	Configures 802.11 DCA list option for outdoor AP.

coverage	Configures 802.11 coverage Hole-Detection.
data fail-percentage *pct*	Configures 802.11 coverage failure-rate threshold for uplink data packets. The range is between 1 and 100
data packet-count *count*	Configures 802.11 coverage minimum-failure-count threshold for uplinkdata packets.
data rssi-threshold *threshold*	Configures 802.11 minimum-receive-coverage level for voice packets.
exception global *percentage*	Configures 802.11 Cisco APs coverage-exception level. The range is between 0 and 100 percent.
level global *number*	Configures 802.11 Cisco AP client-minimum-exception level between 1 and 75 clients.
voice	Configures 802.11 coverage Hole-Detection for voice packets.
fail-percentage *percentage*	Configures 802.11 coverage failure rate threshold for uplink voice packets.
packet-count *number*	Configures 802.11 coverage minimum-uplink-failure count threshold for voice packets.
rssi-threshold *threshold*	Configures 802.11 minimum receive coverage level for voice packets.

Command Default

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

This command applies for both 802.11a and 802.11b bands. But the appropriate commands must be chosen for configuring the parameter.

Examples

This example shows how to configure various RRM settings.

```
Controller#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)#ap dot11 5ghz rrm ?
  ccx             Configure Advanced(RRM) 802.11a CCX options
  channel         Configure advanced 802.11a channel assignment parameters
  coverage        802.11a Coverage Hole Detection
  group-member    Configure members in 802.11a static RF group
  group-mode      802.11a RF group selection mode
  logging         802.11a event logging
  monitor         802.11a statistics monitoring
  ndp-type        Neighbor discovery type Protected/Transparent
  profile         802.11a performance profile
  tpc-threshold   Configures the Tx Power Control Threshold used by RRM for auto
                  power assignment
  txpower         Configures the 802.11a Tx Power Level
```

ap dot11 rrm ccx

To configure radio resource management CCX options for 2.4 GHz and 5GHz devices, use the **ap dot11 rrm ccx** command.

ap dot11 {**24ghz**| **5ghz**} **rrm ccx location-measurement** *interval*

Syntax Description

location-measurement *interval*	Specifies the CCX client-location measurement interval value. The range is between 10 and 32400 seconds.

Command Default

None.

Command Modes

Interface configuration.

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

None.

Examples

This example shows how to set CCX location-measurement interval for a 5-GHz device.

```
Controller#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)#ap dot11 5ghz rrm ccx location-measurement 10
```

ap dot11 rrm channel

To enable radio resource management channel for 2.4 GHz and 5GHz devices, use the **ap dot11 rrm channel** command. To disable the radio resource mangement for 2.4 GHz and 5 GHz devices, use the **no** form of the command.

ap dot11 {**24ghz**| **5ghz**} **rrm channel** {**cleanair-event**| **dca**| **device**| **foreign**| **load**| **noise**}

no ap dot11 {**24ghz**| **5ghz**} **rrm channel** {**cleanair-event**| **dca**| **device**| **foreign**| **load**| **noise**}

Syntax Description

cleanair-event	Specifies the cleanair event-driven RRM parameters
dca	Specifies the 802.11 dynamic channel assignment algorithm parameters
device	Specifies the persistent non-WiFi device avoidance in the 802.11-channel assignment.
foreign	Enables foreign AP 802.11-interference avoidance in the channel assignment.
load	Enables Cisco AP 802.11-load avoidance in the channel assignment.
noise	Enables non-802.11-noise avoidance in the channel assignment.

Command Default

None.

Command Modes

Interface configuration.

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

None.

Examples

This example shows all the parameters available for **Channel**.

```
Controller#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)#ap dot11 24ghz rrm channel ?
  cleanair-event  Configure cleanair event-driven RRM parameters
  dca             Config 802.11b dynamic channel assignment algorithm
                  parameters
  device          Configure persistent non-WiFi device avoidance in the 802.11b
                  channel assignment
  foreign         Configure foreign AP 802.11b interference avoidance in the
```

```
                channel assignment
load            Configure Cisco AP 802.11b load avoidance in the channel
                assignment
noise           Configure 802.11b noise avoidance in the channel assignment
```

ap dot11 rrm coverage

To enable 802.11 coverage hole detection, use the **ap dot11 rrm coverage** command.

ap dot11 {**24ghz**| **5ghz**} **rrm coverage** [**data** {**fail-percentage** *percentage*| **packet-count** *count*| **rssi-threshold** *threshold*}| **exceptional global** *value*| **level global** *value*| **voice** {**fail-percentage** *percentage*| **packet-count** *packet-count*| **rssi-threshold** *threshold*}]

Syntax Description

data	Specifies 802.11 coverage hole-detection data packets.
fail-percentage *percentage*	Specifies 802.11 coverage failure-rate threshold for uplink data packets. The range is between 1 and 100
packet-count *count*	Specifies 802.11 coverage minimum-failure-count threshold for uplink data packets.
rssi-threshold *threshold*	Specifies 802.11 minimum-receive-coverage level for voice packets.
exceptional global *value*	Specifies 802.11 Cisco APs coverage-exception level. The range is between 0 and 100 percent.
level global *value*	Specifies 802.11 Cisco AP client-minimum-exception level between 1 and 75 clients.
voice	Specifies 802.11 coverage Hole-Detection for voice packets.
fail-percentage *percentage*	Specifies 802.11 coverage failure rate threshold for uplink voice packets.
packet-count *packet-count*	Specifies 802.11 coverage minimum-uplink-failure count threshold for voice packets.
rssi-threshold *threshold*	Specifies 802.11 minimum receive coverage level for voice packets.

Command Default

None.

Command Modes

Interface configuration.

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

If you enable coverage hole-detection, the controller automatically determines, based on data that is received from the access points, whether any access points have clients that are potentially located in areas with poor coverage.

If both the number and percentage of failed packets exceed the values that you entered in the **ap dot11 {24ghz | 5ghz} rrm coverage packet-count** and **ap dot11 {24ghz | 5ghz} rrm coverage fail-percentage** commands for a 5-second period, the client is considered to be in a pre-alarm condition. The controller uses this information to distinguish between real and false coverage holes and excludes clients with poor roaming logic. A coverage hole is detected if both the number and percentage of failed clients meet or exceed the values entered in the **ap dot11 {24ghz | 5ghz} rrm coverage level-global** and **ap dot11 {24ghz | 5ghz} rrm coverage exceptional-global** commands over a 90-second period. The controller determines whether the coverage hole can be corrected and, if appropriate, mitigate the coverage hole by increasing the transmit power level for that specific access point.

Examples

This example shows how to set the RSSI-threshold for data in 5-GHz band.

```
Controller#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)#ap dot11 5ghz rrm coverage data rssi-threshold -80
```

ap dot11 rrm group-member

To configure members in 802.11 static RF group, use the **ap dot11 rrm group-member** command. To remove the member, use the **no** form of the command.

ap dot11 {**24ghz**| **5ghz**} **rrm group-member** *controller-name controller-ip*

no ap dot11 {**24ghz**| **5ghz**} **rrm group-member** *controller-name controller-ip*

Syntax Description

controller-name	Specifies the name of the controller to be added.
controller-ip	Specifies the IP address of the controller to be added.

Command Default

None.

Command Modes

Interface configuration.

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

None.

Examples

This example shows how to add a controller in the 5-GHz automatic-RF group

```
Controller#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)#ap dot11 5ghz rrm group-member ABC 10.1.1.1
```

ap dot11 rrm monitor

To monitor the 802.11-band statistics, use the **ap dot11 rrm monitor** command. To disable, use the **no** form of the command.

ap dot11 {**24ghz**| **5ghz**} **rrm monitor** {**channel-list**| {**all**| **country**| **dca**}| **coverage**| **load**| **noise**| **signal**}

no ap dot11 {**24ghz**| **5ghz**} **rrm monitor** {**channel-list**| **coverage**| **load**| **noise**| **signal**}

Syntax Description

channel-list	Sets the 802.11 noise/interference/rogue monitoring channel-list.
all	Specifies to monitor all the channels.
country	Specifies to monitor channels used in configured country code
dca	Specifies to monitor channels used by dynamic channel assignment.
coverage	Specifies 802.11 coverage measurement interval. The range is between 60 and 3600 in seconds
load	Specifies 802.11 load measurement interval. The range is between 60 and 3600 in seconds
noise	Specifies 802.11 noise measurement interval (channel scan interval). The range is between 60 and 3600 in seconds
signal	Specifies 802.11 signal measurement interval (neighbor packet frequency). The range is between 60 and 3600 in seconds

Command Default

None.

Command Modes

Interface Configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

None.

Examples

This example shows how to enable monitoring all the 5-GHz band channels.

```
Controller#configure terminal
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)#ap dot11 5ghz rrm monitor channel-list all
```

ap dot11 rrm profile

To configure Cisco lightweight access point profile settings on supported 802.11 networks, use the **ap dot11 rrm profile** command.

ap dot11 {**24ghz**| **5ghz**} **rrm profile** {**customize**| **foreign** *value*| **noise** *value*| **throughput** *value*| **utilization** *value*}

Syntax Description

customize	Enables performance profiles.
foreign *value*	Specifies the 802.11 foreign 802.11 interference threshold value. The range is between 0 and 100 percent.
noise *value*	Specifies the 802.11 foreign noise threshold value. The range is between -127 and 0 dBm
throughput *value*	Specifies the 802.11a Cisco AP throughput threshold value. The range is between 1000 and 10000000 bytes per second
utilization *value*	Specifies the 802.11a RF utilization threshold value. The range is between 0 and 100 percent

Command Default

Disabled.

Command Modes

Interface configuration.

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

None.

Examples

This example shows how to set the threshold value for the noise parameter.

```
Controller#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)#ap dot11 5ghz rrm profile noise -50
```

ap dot11 rrm tpc-threshold

To configure the tx-power control threshold used by RRM for auto power assignment, use the **ap dot11 rrm tpc-threshold** command. To disable, use the **no** form of the command.

ap dot11 {**24ghz**| **5ghz**} **rrm tpc-threshold** *value*

no ap dot11 {**24ghz**| **5ghz**} **rrm tpc-threshold**

Syntax Description

value	Specifies the power value. The range is between -80 and -50.

Command Default

None.

Command Modes

Interface configuration.

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

None.

Examples

This example shows how to configure the tx-power control threshold used by RRM for auto power assignment.

```
Controller#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)#ap dot11 5ghz rrm tpc-threshold -60
```

ap dot11 rrm txpower

To configures the 802.11 tx-power level, use the **ap dot11 rrm txpower** command.

ap dot11 {**24ghz**| **5ghz**} **rrm txpower** {**auto**| **max** *powerLevel*| **min** *powerLevel*| **once**| *power-level*}

Syntax Description

auto	Enables auto-RF.
max *powerLevel*	Configures maximum auto-RF tx power. The range is between -10 to -30.
min *powerLevel*	Configures minimum auto-RF tx power. The range is between -10 to -30.
once	Enables one-time auto-RF.

Command Default

None.

Command Modes

Interface configuration.

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

None.

Examples

This example shows how to enables auto-RF once.

```
Controller#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)#ap dot11 5ghz rrm txpower once
```

show ap dot11 24ghz

To display the 2.4 GHz RRM parameters, use the **show ap dot11 24ghz** command.

show ap dot11 24ghz {**ccx**| **channel**| **coverage**| **group**| **l2roam**| **logging**| **monitor**| **profile**| **receiver**| **summary**| **txpower**}

Syntax Description

ccx	Displays the 802.11b CCX information for all Cisco APs.
channel	Displays the configuration and statistics of the 802.11b channel assignment.
coverage	Displays the configuration and statistics of the 802.11b coverage.
group	Displays the configuration and statistics of the 802.11b grouping.
l2roam	Displays 802.11b l2roam information.
logging	Displays the configuration and statistics of the 802.11b event logging.
monitor	Displays the configuration and statistics of the 802.11b monitoring.
profile	Displays 802.11b profiling information for all Cisco APs.
receiver	Displays the configuration and statistics of the 802.11b receiver.
summary	Displays the configuration and statistics of the 802.11b Cisco APs.
txpower	Displays the configuration and statistics of the 802.11b transmit power control.

Command Default

None.

Command Modes

Global configuration.

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

None.

Examples

This example shows how to display configuration and statistics of the 802.11b coverage.

```
Controller#show ap dot11 24ghz coverage

Coverage Hole Detection
  802.11b Coverage Hole Detection Mode            : Enabled
  802.11b Coverage Voice Packet Count             : 100 packet(s)
  802.11b Coverage Voice Packet Percentage        : 50%
  802.11b Coverage Voice RSSI Threshold           : -80 dBm
  802.11b Coverage Data Packet Count              : 50 packet(s)
  802.11b Coverage Data Packet Percentage         : 50%
  802.11b Coverage Data RSSI Threshold            : -80 dBm
  802.11b Global coverage exception level         : 25 %
  802.11b Global client minimum exception level   : 3 clients
```

show ap dot11 5ghz

To display the 5GHz RRM parameters, use the **show ap dot11 5ghz** command.

show ap dot11 5ghz {**ccx**| **channel**| **coverage**| **group**| **l2roam**| **logging**| **monitor**| **profile**| **receiver**| **summary**| **txpower**}

Syntax Description

ccx	Displays the 802.11a CCX information for all Cisco APs.
channel	Displays the configuration and statistics of the 802.11a channel assignment.
coverage	Displays the configuration and statistics of the 802.11a coverage.
group	Displays the configuration and statistics of the 802.11a grouping.
l2roam	Displays 802.11a l2roam information.
logging	Displays the configuration and statistics of the 802.11a event logging.
monitor	Displays the configuration and statistics of the 802.11a monitoring.
profile	Displays 802.11a profiling information for all Cisco APs.
receiver	Displays the configuration and statistics of the 802.11a receiver.
summary	Displays the configuration and statistics of the 802.11a Cisco APs.
txpower	Displays the configuration and statistics of the 802.11a transmit power control.

Command Default

None.

Command Modes

Global configuration.

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

None.

Examples

This example shows configuration and statistics of 802.11a channel assignment.

```
Controller#show ap dot11 5ghz channel

Automatic Channel Assignment
  Channel Assignment Mode                     : AUTO
  Channel Update Interval                     : 12 Hours
  Anchor time (Hour of the day)               : 20
  Channel Update Contribution                 : SNI..
  Channel Assignment Leader                   : web (9.9.9.2)
  Last Run                                    : 16534 seconds ago
  DCA Sensitivity Level                       : MEDIUM (15 dB)
  DCA 802.11n Channel Width                   : 40 Mhz
  Channel Energy Levels
      Minimum                                 : unknown
      Average                                 : unknown
      Maximum                                 : unknown
  Channel Dwell Times
      Minimum                                 : unknown
      Average                                 : unknown
      Maximum                                 : unknown
  802.11a 5 GHz Auto-RF Channel List
  Allowed Channel List                        : 36,40,44,48,52,56,60,64,149,153,1

                57,161
  Unused Channel List                         : 100,104,108,112,116,132,136,140,1

                65
  802.11a 4.9 GHz Auto-RF Channel List
  Allowed Channel List                        :
  Unused Channel List                         : 1,2,3,4,5,6,7,8,9,10,11,12,13,14,

                15,16,17,18,19,20,21,22,23,24,25,26
  DCA Outdoor AP option                       : Disabled
```

PART XI

Lightweight Access Points

Cisco Lightweight Access Point Commands

ap auth-list ap-policy

To configure authorization policy for all Cisco lightweight access points joined to the controller, use the **ap auth-list ap-policy** command. To disable authorization policy for all Cisco lightweight access points joined to the controller, use the **no** form of this command.

ap auth-list ap-policy {**authorize-ap| authorize-lsc-ap| lsc| mic| ssc**}

no ap auth-list ap-policy {**authorize-ap| authorize-lsc-ap| lsc| mic| ssc**}

Syntax Description

authorize-ap	Enables the authorization policy.
authorize-lsc-ap	Enables the locally significant certificate authorization policy.
lsc	Enables access points with locally significant certificates to connect.
mic	Enables access points with manufacture-installed certificates to connect.
ssc	Enables access points with self signed certificates to connect.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to enable the access point authorization policy:

```
Controller(config)# ap auth-list ap-policy authorize-ap
```

This example shows how to enable the locally significant certificate authorization policy:

```
Controller(config)# ap auth-list ap-policy authorize-lsc-ap
```

This example shows how to enable access points with locally significant certificates to connect:

```
Controller(config)# ap auth-list ap-policy lsc
```

This example shows how to enable access points with manufacture-installed certificates to connect:

```
Controller(config)# ap auth-list ap-policy mic
```

This example shows how to enable access points with self-signed certificates to connect:

```
Controller(config)# ap auth-list ap-policy ssc
```

ap bridging

To enable Ethernet to 802.11 bridging on a Cisco lightweight access point, use the **ap bridging** command. To disable Ethernet to 802.11 bridging on a Cisco lightweight access point, use the **no** form of this command.

ap bridging

no ap bridging

Syntax Description

This command has no keywords and arguments.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to enable Ethernet-to-Ethernet bridging on a lightweight access point:

```
Controller(config)# ap bridging
```

This example shows how to disable Ethernet-to-Ethernet bridging on a lightweight access point:

```
Controller(config)# no ap bridging
```

ap capwap backup

To configure a primary or secondary backup controller for all access points that are joined to a specific controller, use the **ap capwap backup** command.

ap capwap backup {**primary** *primary-controller-name primary-controller-ip-address* | **secondary** *secondary-controller-name secondary-controller-ip-address*}

Syntax Description

primary	Specifies the primary backup controller.
primary-controller-name	Primary backup controller name.
primary-controller-ip-address	Primary backup controller IP address.
secondary	Specifies the secondary backup controller.
secondary-controller-name	Secondary backup controller name.
secondary-controller-ip-address	Secondary backup controller IP address.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to configure a primary backup controller for all access points that are joined to a specific controller:

```
Controller(config)# ap capwap backup primary controller1 192.0.2.51
```

This example shows how to configure a secondary backup controller for all access points that are joined to a specific controller:

```
Controller(config)# ap capwap backup secondary controller1 192.0.2.52
```

ap capwap multicast

To configure the multicast address used by all access points to receive multicast traffic when multicast forwarding is enabled and to configure the outer Quality of Service (QoS) level of those multicast packets sent to the access points, use the **ap capwap multicast** command.

ap capwap multicast {*multicast-ip-address*| **service-policy output** *pollicymap-name*}

Syntax Description

multicast-ip-address	Multicast IP address.
service-policy	Specifies the tunnel QoS policy for multicast access points.
output	Assigns a policy map name to the output.
policymap-name	Service policy map name.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to configure a multicast address used by all access points to receive multicast traffic when multicast forwarding is enabled:

```
Controller(config)# ap capwap multicast 239.2.2.2
```

This example shows how to configure a tunnel multicast QoS service policy for multicast access points:

```
Controller(config)# ap capwap multicast service-policy output tunnmulpolicy
```

ap capwap retransmit

To configure Control and Provisioning of Wireless Access Points (CAPWAP) control packet retransmit count and control packet retransmit interval, use the **ap capwap retransmit** command.

ap capwap retransmit {**count** *retransmit-count*| **interval** *retransmit-interval*}

Syntax Description

count *retransmit-count*	Specifies the access point CAPWAP control packet retransmit count. **Note** The count is from 3 to 8 seconds.
interval *retransmit-interval*	Specifies the access point CAPWAP control packet retransmit interval. **Note** The interval is from 2 to 5 seconds.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to configure the CAPWAP control packet retransmit count for an access point:

```
Controller# ap capwap retransmit count 3
```

This example shows how to configure the CAPWAP control packet retransmit interval for an access point:

```
Controller# ap capwap retransmit interval 5
```

ap capwap timers

To configure advanced timer settings, use the **ap capwap timers** command.

ap capwap timers {**discovery-timeout** *seconds*| **fast-heartbeat-timeout local** *seconds*| **heartbeat-timeout** *seconds*| **primary-discovery-timeout** *seconds*| **primed-join-timeout** *seconds*}

Syntax Description

discovery-timeout	Specifies the Cisco lightweight access point discovery timeout. **Note** The Cisco lightweight access point discovery timeout is how long a Cisco controller waits for an unresponsive access point to answer before considering that the access point failed to respond.
seconds	Cisco lightweight access point discovery timeout from 1 to 10 seconds. **Note** The default is 10 seconds.
fast-heartbeat-timeout local	Enables the fast heartbeat timer that reduces the amount of time it takes to detect a controller failure for local or all access points.
seconds	Small heartbeat interval (from 1 to 10 seconds) that reduces the amount of time it takes to detect a controller failure. **Note** The fast heartbeat time-out interval is disabled by default.
heartbeat-timeout	Specifies the Cisco lightweight access point heartbeat timeout. **Note** The Cisco lightweight access point heartbeat timeout controls how often the Cisco lightweight access point sends a heartbeat keep-alive signal to the Cisco controller. This value should be at least three times larger than the fast heartbeat timer.
seconds	Cisco lightweight access point heartbeat timeout value from 1 to 30 seconds. **Note** The default is 30 seconds.
primary-discovery-timeout	Specifies the access point primary discovery request timer. The timer determines the amount of time taken by an access point to discovery the configured primary, secondary, or tertiary controller.
seconds	Access point primary discovery request timer from 30 to 3600 seconds. **Note** The default is 120 seconds.
primed-join-timeout	Specifies the authentication timeout. Determines the time taken by an access point to determine that the primary controller has become unresponsive. The access point makes no further attempts to join the controller until the connection to the controller is restored.

seconds	Authentication response timeout from 120 to 43200 seconds. **Note** The default is 120 seconds.

Command Default None

Command Modes Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples This example shows how to configure an access point discovery timeout with the timeout value of 7:

```
Controller(config)# ap capwap timers discovery-timeout 7
```

This example shows how to enable the fast heartbeat interval for all access points:

```
Controller(config)# ap capwap timers fast-heartbeat-timeout 6
```

This example shows how to configure an access point heartbeat timeout to 20:

```
Controller(config)# ap capwap timers heartbeat-timeout 20
```

This example shows how to configure the access point primary discovery request timer to 1200 seconds:

```
Controller(config)# ap capwap timers primary-discovery-timeout 1200
```

This example shows how to configure the authentication timeout to 360 seconds:

```
Controller(config)# ap capwap timers primed-join-timeout 360
```

ap cdp

To enable the Cisco Discovery Protocol (CDP) on a Cisco lightweight access point, use the **ap cdp** command. To disable the Cisco Discovery Protocol (CDP) on a Cisco lightweight access point, use the **no** form of this command.

ap cdp [**interface** {**ethernet** *ethernet-id*| **radio** *radio-id*}]

no ap cdp [**interface** {**ethernet** *ethernet-id*| **radio** *radio-id*}]

Syntax Description

interface	(Optional) Specifies CDP in a specific interface.
ethernet	Specifies CDP for an Ethernet interface.
ethernet-id	Ethernet interface number from 0 to 3.
radio	Specifies CDP for a radio interface.
radio-id	Radio number from 0 to 3.

Command Default

Disabled on all access points.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The **no ap cdp** command disables CDP on all access points that are joined to the controller and all access points that join in the future. CDP remains disabled on both current and future access points even after the controller or access point reboots. To enable CDP, enter the **ap cdp** command.

Note CDP over Ethernet/radio interfaces is available only when CDP is enabled. After you enable CDP on all access points joined to the controller, you can disable and then reenable CDP on individual access points using the **ap name** *Cisco-AP* **cdp** command. After you disable CDP on all access points joined to the controller, you can enable and then disable CDP on individual access points.

Examples

This example shows how to enable CDP on all access points:

```
Controller(config)# ap cdp
```

This example shows how to enable CDP for Ethernet interface number 0 on all access points:

```
Controller(config)# ap cdp ethernet 0
```

ap core-dump

To enable a Cisco lightweight access point's memory core dump settings, use the **ap core-dump** command. To disable a Cisco lightweight access point's memory core dump settings, use the **no** form of this command.

ap core-dump *tftp-ip-addr filename* {**compress**| **uncompress**}

no ap core-dump

Syntax Description

tftp-ip-addr	IP address of the TFTP server to which the access point sends core dump files.
filename	Name that the access point uses to label the core file.
compress	Compresses the core dump file.
uncompress	Uncompresses the core dump file.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The access point must be able to reach the TFTP server.

Examples

This example shows how to configure and compress the core dump file:

```
Controller(config)# ap core-dump 192.0.2.51 log compress
```

ap country

To configure one or more country codes for a controller, use the **ap country** command.

ap country *country-code*

Syntax Description

country-code	Two-letter or three-letter country code or several country codes separated by a comma.

Command Default

US (country code of the United States of America).

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The Cisco controller must be installed by a network administrator or qualified IT professional and the installer must select the proper country code. Following installation, access to the unit should be password protected by the installer to maintain compliance with regulatory requirements and to ensure proper unit functionality. See the related product guide for the most recent country codes and regulatory domains.

Examples

This example shows how to configure country codes on the controller to IN (India) and FR (France):

```
Controller(config)# ap country IN,FR
```

ap crash-file

To delete crash and radio core dump files, use the **ap crash-file** command.

ap crash-file {**clear-all**| **delete** *filename*}

Syntax Description

clear-all	Deletes all the crash and radio core dump files.
delete	Deletes a single crash and radio core dump file.
filename	Name of the file to delete.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to delete all crash files:

```
Controller# ap crash-file clear-all
```

This example shows how to delete crash file 1:

```
Controller# ap crash-file delete crash-file-1
```

ap dot11 24ghz preamble

To enable only a short preamble as defined in subclause 17.2.2.2 , use the **ap dot11 24ghz preamble** command. To enable long preambles (for backward compatibility with pre-802.11b devices, if these devices are still present in your network) or short preambles (recommended unless legacy pre-802.11b devices are present in the network), use the **no** form of this command.

ap dot11 24ghz preamble short

no ap dot11 24ghz preamble short

Syntax Description

short	Specifies the short 802.11b preamble.

Command Default

short preambles

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Note You must reboot the Cisco controller (reset system) with the **Save** command before you can use the **ap dot11 24ghz preamble** command.

This parameter may need to be set to long to optimize this Cisco controller for some legacy clients, including SpectraLink NetLink telephones.

This command can be used any time that the CLI interface is active.

Examples

This example shows how to enable both long and short preamblest:

```
Controller(config)# no ap dot11 24ghz preamble short
```

ap dot11 24ghz dot11g

To enable the Cisco wireless LAN solution 802.11g network, use the **ap dot11 24ghz dot11g** command. To disable the Cisco wireless LAN solution 802.11g network, use the **no** form of this command.

ap dot11 24ghz dot11g

no ap dot11 24ghz dot11g

Syntax Description

This command has no keywords and arguments.

Command Default

Enabled

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Before you enter the **ap dot11 24ghz dot11g** command, disable the 802.11 Cisco radio with the **ap dot11 24ghz shutdown** command.

After you configure the support for the 802.11g network, use the **no ap dot11 24ghz shutdown** command to enable the 802.11 2.4 Ghz radio.

Examples

This example shows how to enable the 802.11g network:

```
Controller(config)# ap dot11 24ghz dot11g
```

ap dot11 5ghz channelswitch mode

To configure a 802.11h channel switch announcement, use the **ap dot11 5ghz channelswitch mode** command. To disable a 802.11h channel switch announcement, use the **no** form of this command.

ap dot11 5ghz channelswitch mode *value*

no ap dot11 5ghz channelswitch mode

Syntax Description

value	802.11h channel announcement value. **Note** You can specify anyone of the following two values: • 0—Indicates that the channel switch announcement is disabled. • 1—Indicates that the channel switch announcement is enabled.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to enable the 802.11h switch announcement:

```
Controller(config)# ap dot11 5ghz channelswitch mode 1
```

ap dot11 5ghz power-constraint

To configure the 802.11h power constraint value, use the **ap dot11 5ghz power-constraint** command. To remove the 802.11h power constraint value, use the **no** form of this command.

ap dot11 5ghz power-constraint *value*

no ap dot11 5ghz power-constraint

Syntax Description

value	802.11h power constraint value. **Note** The range is from 0 to 30 dBm.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to configure the 802.11h power constraint to 5 dBm:

```
Controller(config)# ap dot11 5ghz power-constraint 5
```

ap dot11 beaconperiod

To change the beacon period globally for 2.4 GHz or 5 GHz bands, use the **ap dot11 beaconperiod** command.

Note Disable the 802.11 network before using this command. See the "Usage Guidelines" section.

ap dot11 {**24ghz**| **5ghz**} **beaconperiod** *time*

Syntax Description

24ghz	Specifies the settings for 2.4 GHz band.
5ghz	Specifies the settings for 5 GHz band.
beaconperiod	Specifies the beacon for a network globally.
time	Beacon interval in time units (TU). One TU is 1024 microseconds. The range is from 20 to 1000.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

In Cisco wireless LAN 802.11 networks, all Cisco lightweight access point wireless LANs broadcast a beacon at regular intervals. This beacon notifies clients that the wireless service is available and allows the clients to synchronize with the lightweight access point.

Before you change the beacon period, make sure that you have disabled the 802.11 network by using the **ap dot11** {**24ghz | 5ghz**} **shutdown** command. After changing the beacon period, enable the 802.11 network by using the **no ap dot11** {**24ghz | 5ghz**} **shutdown** command.

Examples

This example shows how to configure the 5 GHZ band for a beacon period of 120 time units:

```
Controller(config)# ap dot11 5ghz beaconperiod 120
```

ap dot11 beamforming

To enable beamforming on the network or on individual radios, use the **ap dot11 beamforming** command.

ap dot11 {**24ghz**| **5ghz**} **beamforming**

Syntax Description

24ghz	Specifies the 2.4 GHz band.
5ghz	Specifies the 5 GHz band.
beamforming	Specifies beamforming on the network.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

When you enable beamforming on the network, it is automatically enabled for all the radios applicable to that network type.

Follow these guidelines for using beamforming:

- Beamforming is supported for legacy orthogonal frequency-division multiplexing (OFDM) data rates (6, 9, 12, 18, 24, 36, 48, and 54 Mbps).

  Note Beamforming is not supported for Direct Sequence Spread Spectrum data rates (1 and 2 Mbps) and Complementary-Code Key (CCK) data rates (5.5 and 11 Mbps).

- Beamforming is supported only on access points that support 802.11n (AP1260, AP3500, and AP3600).
- Two or more antennas must be enabled for transmission.
- All three antennas must be enabled for reception.
- OFDM rates must be enabled.

  If the antenna configuration restricts operation to a single transmit antenna, or if OFDM rates are disabled, beamforming is not used.

Examples

This example shows how to enable beamforming on the 5 GHz band:

```
Controller(config)# ap dot11 5ghz beamforming
```

ap dot11 cac media-stream

To configure media stream Call Admission Control (CAC) voice and video quality parameters for 2.4 GHz and 5 GHz bands, use the **ap dot11 cac media-stream** command.

ap dot11 {**24ghz**| **5ghz**} **cac media-stream multicast-direct** {**max-retry-percent** *retryPercent*| **min-client-rate**{**eighteen**| **eleven**| **fiftyFour**| **fivePointFive**| **fortyEight**| **nine**| **oneFifty**| **oneFortyFourPointFour**| **oneThirty**| **oneThirtyFive**| **seventyTwoPointTwo**| **six**| **sixtyFive**| **thirtySix**| **threeHundred**| **twelve**| **twentyFour**| **two**| **twoSeventy**}}

Syntax Description

24ghz	Specifies the 2.4 GHz band.
5ghz	Specifies the 5 GHz band.
multicast-direct	Specifies CAC parameters for multicast-direct media streams.
max-retry-percent	Specifies the percentage of maximum retries that are allowed for multicast-direct media streams.
retryPercent	Percentage of maximum retries that are allowed for multicast-direct media streams. **Note** The range is from 0 to 100.
min-client-rate	Specifies the minimum transmission data rate to the client for multicast-direct media streams (rate at which the client must transmit in order to receive multicast-direct unicast streams). If the transmission rate is below this rate, either the video will not start or the client may be classified as a bad client. The bad client video can be demoted for better effort QoS or subject to denial.

min-client-rate	You can choose the following rates: • **eighteen** • **eleven** • **fiftyFour** • **fivePointFive** • **fortyEight** • **nine** • **one** • **oneFifty** • **oneFortyFourPointFour** • **oneThirty** • **oneThirtyFive** • **seventyTwoPointTwo** • **six** • **sixtyFive** • **thirtySix** • **threeHundred** • **twelve** • **twentyFour** • **two** • **twoSeventy**

Command Default

The default value for the maximum retry percent is 80. If it exceeds 80, either the video will not start or the client might be classified as a bad client. The bad client video will be demoted for better effort QoS or is subject to denial.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

CAC commands require that the WLAN you are planning to modify is configured for the Wi-Fi Multimedia (WMM) protocol.

Before you can configure CAC parameters on a network, you must complete the following prerequisites:

- Disable all WLANs with WMM enabled by entering the **wlan** *wlan_name* **shutdown** command.
- Disable the radio network you want to configure by entering the **ap dot11** {**24ghz | 5ghz**} **shutdown** command.
- Save the new configuration.
- Enable voice or video CAC for the network you want to configure by entering the **ap dot11** {**24ghz | 5ghz**} **cac voice acm** or **ap dot11** {**24ghz | 5ghz**} **cac video acm** commands.

Examples

This example shows how to configure the maximum retry percent for multicast-direct media streams as 90 on a 802.11a network:

```
Controller(config)# ap dot11 5ghz cac media-stream multicast max-retry-percent 90
```

ap dot11 cac multimedia

To configure multimedia Call Admission Control (CAC) voice and video quality parameters for 2.4 GHz and 5 GHz bands, use the **ap dot11 cac multimedia** command.

ap dot11 {**24ghz**| **5ghz**} **cac multimedia max-bandwidth** *bandwidth*

Syntax Description

24ghz	Specifies the 2.4 GHz band.
5ghz	Specifies the 5 GHz band.
max-bandwidth	Specifies the percentage of maximum bandwidth allocated to Wi-Fi Multimedia (WMM) clients for voice and video applications on the 2.4 GHz or 5 GHz band.
bandwidth	Percentage of the maximum bandwidth allocated to WMM clients for voice and video applications on the 802.11a or 802.11b/g network. Once the client reaches the specified value, the access point rejects new multimedia flows this radio band. The range is from 5 to 85%.

Command Default

The default value is 75%.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

CAC commands require that the WLAN you are planning to modify is configured for the Wi-Fi Multimedia (WMM) protocol.

Before you can configure CAC parameters on a network, you must complete the following prerequisites:

- Disable all WLANs with WMM enabled by entering the **wlan** *wlan_name* **shutdown** command.
- Disable the radio network you want to configure by entering the **ap dot11** {**24ghz | 5ghz**} **shutdown** command.
- Save the new configuration.
- Enable voice or video CAC for the network you want to configure by entering the **ap dot11** {**24ghz | 5ghz**} **cac voice acm** or **ap dot11** {**24ghz | 5ghz**} **cac video acm** commands.

Examples

This example shows how to configure the percentage of the maximum bandwidth allocated to WMM clients for voice and video applications on the 5 GHz band:

```
Controller(config)# ap dot11 5ghz cac multimedia max-bandwidth 5
```

ap dot11 cac video

To configure Call Admission Control (CAC) parameters for the video category, use the **ap dot11 cac video** command. To disable the CAC parameters for video category, use the **no** form of this command.

ap dot11 {**24ghz**| **5ghz**} **cac video** {**acm**| **max-bandwidth** *value*| **roam-bandwidth** *value*}

no ap dot11 {**24ghz**| **5ghz**} **cac video** {**acm**| **max-bandwidth** *value*| **roam-bandwidth** *value*}

Syntax Description

24ghz	Specifies the 2.4 GHz band.
5ghz	Specifies the 5 GHz band.
acm	Enables bandwidth-based video CAC for the 2.4 GHz or 5 GHz band. **Note** To disable bandwidth-based video CAC for the 2.4 GHz or 5 GHz band, use the **no ap dot11** {**24ghz | 5ghz**} **cac video acm** command.
max-bandwidth	Sets the percentage of the maximum bandwidth allocated to clients for video applications on the 2.4 GHz or 5 GHz band.
value	Bandwidth percentage value from 5 to 85%.
roam-bandwidth	Sets the percentage of the CAC maximum allocated bandwidth reserved for roaming video clients on the 2.4 GHz or 5 GHz band.
value	Bandwidth percentage value from 0 to 85%.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

CAC commands require that the WLAN you are planning to modify is configured for the Wi-Fi Multimedia (WMM) protocol.

Before you can configure CAC parameters on a network, you must complete the following prerequisites:

- Disable all WLANs with WMM enabled by entering the **wlan** *wlan_name* **shutdown** command.
- Disable the radio network you want to configure by entering the **ap dot11** {**24ghz | 5ghz**} **shutdown** command.

- Save the new configuration.
- Enable voice or video CAC for the network you want to configure by entering the **ap dot11** {**24ghz | 5ghz**} **cac voice acm** or **ap dot11** {**24ghz | 5ghz**} **cac video acm** command.

Examples

This example shows how to enable the bandwidth-based CAC:

```
Controller(config)# ap dot11 24ghz cac video acm
```

This example shows how to specify the percentage of the maximum allocated bandwidth for video applications on the selected radio band:

```
Controller(config)# ap dot11 24ghz cac video max-bandwidth 50
```

This example shows how to configure the percentage of the maximum allocated bandwidth reserved for roaming video clients on the selected radio band:

```
Controller(config)# ap dot11 24ghz cac video roam-bandwidth 10
```

ap dot11 cac voice

To configure Call Admission Control (CAC) parameters for the voice category, use the **ap dot11 cac voice** command.

ap dot11 {**24ghz**| **5ghz**} **cac voice**{**acm**| **load-based**| **max-bandwidth** *value*| **roam-bandwidth** *value*| **sip** [**bandwidth** *bw*] **sample-interval** *value*| **stream-size** *x* **max-streams** *y*| **tspec-inactivity-timeout**{**enable**| **ignore**}}

Syntax Description

24ghz	Specifies the 2.4 GHz band.
5ghz	Specifies the 5 GHz band.
acm	Enables bandwidth-based voice CAC for the 2.4 GHz or 5 GHz band. **Note** To disable bandwidth-based voice CAC for the 2.4 GHz or 5 GHz band, use the **no ap dot11** {**24ghz | 5ghz**} **cac voice acm** command.
load-based	Enable load-based CAC on voice access category. **Note** To disable load-based CAC on voice access category for the 2.4 GHz or 5 GHz band, use the **no ap dot11** {**24ghz | 5ghz**} **cac voice load-based** command.
max-bandwidth	Sets the percentage of the maximum bandwidth allocated to clients for voice applications on the 2.4 GHz or 5 GHz band.
value	Bandwidth percentage value from 5 to 85%.
roam-bandwidth	Sets the percentage of the CAC maximum allocated bandwidth reserved for roaming voice clients on the 2.4 GHz or 5 GHz band.
value	Bandwidth percentage value from 0 to 85%.
sip	Specifies the CAC codec name and sample interval as parameters and calculates the required bandwidth per call for the 802.11 networks.
bandwidth	(Optional) Specifies bandwidth for a SIP-based call.

bw	Bandwidth in kbps. The following bandwidth values specify parameters for the SIP codecs: • 64kbps—Specifies CAC parameters for the SIP G711 codec. • 8kbps—Specifies CAC parameters for the SIP G729 codec. **Note** The default value is 64 Kbps.
sample-interval	Specifies the packetization interval for SIP codec.
value	Packetization interval in msecs. The sample interval for SIP codec value is 20 seconds.
stream-size	Specifies the number of aggregated voice Wi-Fi Multimedia (WMM) traffic specification (TSPEC) streams at a specified data rate for the 2.4 GHz or 5 GHz band.
x	Stream size. The range of the stream size is from 84000 to 92100.
max-streams	Specifies the maximum number of streams per TSPEC.
y	Number (1 to 5) of voice streams. **Note** The default number of streams is 2 and the mean data rate of a stream is 84 kbps.
tspec-inactivity-timeout	Specifies TSPEC inactivity timeout processing mode. **Note** Use this keyword to process or ignore the Wi-Fi Multimedia (WMM) traffic specifications (TSPEC) inactivity timeout received from an access point. When the inactivity timeout is ignored, a client TSPEC is not deleted even if the access point reports an inactivity timeout for that client.
enable	Processes the TSPEC inactivity timeout messages.
ignore	Ignores the TSPEC inactivity timeout messages. **Note** The default is **ignore** (disabled).

Command Default None

Command Modes Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

CAC commands require that the WLAN you are planning to modify is configured for the Wi-Fi Multimedia (WMM) protocol and the quality of service (QoS) level be set to Platinum.

Before you can configure CAC parameters on a network, you must complete the following prerequisites:

- Disable all WLANs with WMM enabled by entering the **wlan** *wlan_name* **shutdown** command.
- Disable the radio network you want to configure by entering the **ap dot11** {**24ghz | 5ghz**} **shutdown** command.
- Save the new configuration.
- Enable voice or video CAC for the network you want to configure by entering the **ap dot11** {**24ghz | 5ghz**} **cac voice acm** or **ap dot11** {**24ghz | 5ghz**} **cac video acm** commands.

Examples

This example shows how to enable the bandwidth-based CAC:

```
Controller(config)# ap dot11 24ghz cac voice acm
```

This example shows how to enable the load-based CAC on the voice access category:

```
Controller(config)# ap dot11 24ghz cac voice load-based
```

This example shows how to specify the percentage of the maximum allocated bandwidth for voice applications on the selected radio band:

```
Controller(config)# ap dot11 24ghz cac voice max-bandwidth 50
```

This example shows how to configure the percentage of the maximum allocated bandwidth reserved for roaming voice clients on the selected radio band:

```
Controller(config)# ap dot11 24ghz cac voice roam-bandwidth 10
```

This example shows how to configure the bandwidth and voice packetization interval for the G729 SIP codec on a 2.4 GHz band:

```
Controller(config)# ap dot11 24ghz cac voice sip bandwidth 8 sample-interval 40
```

This example shows how to configure the number of aggregated voice traffic specifications stream with a stream size of 85000 and with a maximum of 5 streams:

```
Controller(config)# ap dot11 24ghz cac voice stream-size 85000 max-streams 5
```

This example shows how to enable the voice TSPEC inactivity timeout messages received from an access point:

```
Controller(config)# ap dot11 24ghz cac voice tspec-inactivity-timeout enable
```

ap dot11 cleanair

To configure CleanAir on 802.11 networks, use the **ap dot11 cleanair** command. To disable CleanAir on 802.11 networks, use the **no** form of this command.

ap dot11 {**24ghz**| **5ghz**} **cleanair**

no ap dot11 {**24ghz**| **5ghz**} **cleanair**

Syntax Description

24ghz	Specifies the 2.4 GHz band.
5ghz	Specifies the 5 GHz band.
cleanair	Specifies CleanAir on the 2.4 GHz or 5 GHz band.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to enable the CleanAir settings on the 2.4 GHz band:

```
Controller(config)# ap dot11 24ghz cleanair
```

ap dot11 cleanair alarm air-quality

To configure CleanAir air-quality alarms for Cisco lightweight access points, use the **ap dot11 cleanair alarm air-quality** command.

ap dot11 {**24ghz**| **5ghz**} **cleanair alarm air-quality** [**threshold** *value*]

Syntax Description

24ghz	Specifies the 2.4 GHz band.
5ghz	Specifies the 5 GHz band.
threshold	Specifies the air-quality alarm threshold.
value	Air quality alarm threshold (1 is bad air quality, and 100 is good air quality).

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to configure the CleanAir 2.4 GHz air-quality threshold to 90:

```
Controller(config)# ap dot11 24ghz cleanair air-quality threshold 90
```

ap dot11 cleanair alarm device

To configure the CleanAir interference devices alarms on the 2.4 GHz or 5 GHz bands, use the **ap dot11 cleanair alarm device** command. To disable the CleanAir interference devices alarms on the 802.11 networks, use the **no** form of this command.

ap dot11 {**24ghz**| **5ghz**} **cleanair alarm device**{**all**| **bt-discovery**| **bt-link**| **canopy**| **cont-tx**| **dect-like**| **fh**| **inv**| **jammer**| **mw-oven**| **nonstd**| **superag**| **tdd-tx**| **video**| **wimax-fixed**| **wimax-mobile**| **xbox**| **zigbee**}

no ap dot11 {**24ghz**| **5ghz**} **cleanair**

Syntax Description

24ghz	Specifies the 2.4 GHz band.
5ghz	Specifies the 5 GHz band.
all	Specifies all the device types at once.
bt-discovery	Specifies the Bluetooth device in discovery mode.
bt-link	Specifies the Bluetooth active link.
canopy	Specifies the Canopy devices.
cont-tx	Specifies the continuous transmitter.
dect-like	Specifies a Digital Enhanced Cordless Communication (DECT)-like phone.
fh	Specifies the frequency hopping devices.
inv	Specifies the devices using spectrally inverted Wi-Fi signals.
jammer	Specifies the jammer.
mw-oven	Specifies the microwave oven devices.
nonstd	Specifies the devices using nonstandard Wi-Fi channels.
superag	Specifies 802.11 SuperAG devices.
tdd-tx	Specifies the TDD transmitter.
video	Specifies video cameras.
wimax-fixed	Specifies a WiMax fixed device.
wimax-mobile	Specifies a WiMax mobile device.
xbox	Specifies the Xbox device.

zigbee	Specifies the ZigBee device.

Command Default Disabled

Command Modes Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples This example shows how to disable alarms for ZigBee interference detection:

```
Controller(config)# no ap dot11 24ghz cleanair alarm device zigbee
```

This example shows how to enable alarms for detection of Bluetooth links:

```
Controller(config)# ap dot11 24ghz cleanair alarm device bt-link
```

ap dot11 cleanair device

To configure CleanAir interference device types, use the **ap dot11 cleanair device** command.

ap dot11 24ghz cleanair device [**all**| **bt-discovery**| **bt-link**| **canopy**| **cont-tx**| **dect-like**| **fh**| **inv**| **jammer**| **mw-oven**| **nonstd**| **superag**| **tdd-tx**| **video**| **wimax-fixed**| **wimax-mobile**| **xbox**| **zigbee**]

Syntax Description

all	Specifies all device types.
device	Specifies the CleanAir interference device type.
bt-discovery	Specifies the Bluetooth device in discovery mode.
bt-link	Specifies the Bluetooth active link.
canopy	Specifies the Canopy devices.
cont-tx	Specifies the continuous transmitter.
dect-like	Specifies a Digital Enhanced Cordless Communication (DECT)-like phone.
fh	Specifies the 802.11 frequency hopping devices.
inv	Specifies the devices using spectrally inverted Wi-Fi signals.
jammer	Specifies the jammer.
mw-oven	Specifies the microwave oven devices.
nonstd	Specifies the devices using nonstandard Wi-Fi channels.
superag	Specifies 802.11 SuperAG devices.
tdd-tx	Specifies the TDD transmitter.
video	Specifies video cameras.
wimax-fixed	Specifies a WiMax fixed device.
wimax-mobile	Specifies a WiMax mobile device.
xbox	Specifies the Xbox device.
zigbee	Specifies the ZigBee device.

Command Default

None

Command Modes Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples This example shows how to configure the controller to monitor ZigBee interferences:

```
Controller(config)# ap dot11 24ghz cleanair device zigbee
```

ap dot11 dot11n

To configure settings for an 802.11n network, use the **ap dot11 dot11n** command.

ap dot11 {**24ghz**| **5ghz**} **dot11n** {**a-mpdu tx priority**{*priority_value*| **all**}| **a-msdu tx priority**{*priority_value*| **all**}| **guard-interval** {**any**| **long**}| **mcs tx** *rate*| **rifs rx**}

Syntax Description

24ghz	Specifies the 2.4 GHz band.
5ghz	Specifies the 5 GHz band.
dot11n	Enables 802.11n support.
a-mpdu tx priority	Specifies the traffic that is associated with the priority level that uses A-MPDU transmission.
priority_value	Aggregated MAC protocol data unit priority level from 0 to 7.
all	Specifies all of the priority levels at once.
a-msdu tx priority	Specifies the traffic that is associated with the priority level that uses A-MSDU transmission.
priority_value	Aggregated MAC protocol data unit priority level from 0 to 7.
all	Specifies all of the priority levels at once.
guard-interval	Specifies the guard interval.
any	Enables either a short or a long guard interval.
long	Enables only a long guard interval.
mcs tx *rate*	Specifies the modulation and coding scheme (MCS) rates at which data can be transmitted between the access point and the client.
rate	Specifies the modulation and coding scheme data rates. **Note** The range is from 0 to 23.
rifs rx	Specifies the Reduced Interframe Space (RIFS) between data frames.

Command Default

By default, priority 0 is enabled.

Command Modes Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines Aggregation is the process of grouping packet data frames together rather than transmitting them separately. Two aggregation methods are available: Aggregated MAC Protocol Data Unit (A-MPDU) and Aggregated MAC Service Data Unit (A-MSDU). A-MPDU is performed in the software; A-MSDU is performed in the hardware.

Aggregated MAC Protocol Data Unit priority levels assigned per traffic type are as follows:

- 0—Best effort
- 1—Background
- 2—Spare
- 3—Excellent effort
- 4—Controlled load
- 5—Video, less than 100-ms latency and jitter
- 6—Voice, less than 10-ms latency and jitter
- 7—Network control
- all—Configure all of the priority levels at once.

Note Configure the priority levels to match the aggregation method used by the clients.

Examples This example shows how to enable 802.11n support on a 2.4 GHz band:

```
Controller(config)# ap dot11 24ghz dot11n
```

This example shows how to configure all the priority levels at once so that the traffic that is associated with the priority level uses A-MSDU transmission:

```
Controller(config)# ap dot11 24ghz dot11n a-msdu tx priority all
```

This example shows how to enable only long guard intervals:

```
Controller(config)# ap dot11 24ghz dot11n guard-interval long
```

This example shows how to specify MCS rates:

```
Controller(config)# ap dot11 24ghz dot11n mcs tx 5
```

This example shows how to enable RIFS:

```
Controller(config)# ap dot11 24ghz dot11n rifs rx
```

ap dot11 dtpc

To configure Dynamic Transmit Power Control (DTPC) settings, Cisco Client eXtension (CCX) version 5 expedited bandwidth request feature, and the fragmentation threshold on an 802.11 network, use the **ap dot11 dtpc** command.

ap dot11 {**24ghz**| **5ghz**} {**dtpc**| **exp-bwreq**| **fragmentation** *threshold*}

Syntax Description

24ghz	Specifies the 2.4 GHz band.
5ghz	Specifies the 5 GHz band.
dtpc	Specifies Dynamic Transport Power Control (DTPC) settings. **Note** This option is enabled by default.
exp-bwreq	Specifies Cisco Client eXtension (CCX) version 5 expedited bandwidth request feature. **Note** The expedited bandwidth request feature is disabled by default.
fragmentation *threshold*	Specifies the fragmentation threshold. **Note** This option can only used be when the network is disabled using the **ap dot11** {**24ghz** | **5ghz**} **shutdown** command.
threshold	Threshold. The range is from 256 to 2346 bytes (inclusive).

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

When the CCX version 5 expedited bandwidth request feature is enabled, the controller configures all joining access points for this feature.

Examples

This example shows how to enable DTPC for the 5 GHz band:

```
Controller(config)# ap dot11 5ghz dtpc
```

This example shows how to enable the CCX expedited bandwidth settings:

```
Controller(config)# ap dot11 5ghz exp-bwrep
```

This example shows how to configure the fragmentation threshold on the 5 GHz band with the threshold number of 1500 bytes:

```
Controller(config)# ap dot11 5ghz fragmentation 1500
```

ap dot11 edca-parameters

To enable a specific enhanced distributed channel access (EDCA) profile on the 2.4 GHz or 5 GHz bands, use the **ap dot11 edca-parameters** command. To disable an EDCA profile on the 2.4 GHz or 5 GHz bands, use the **no** form of this command.

ap dot11 {**24ghz**| **5ghz**} **edca-parameters** {**custom-voice**| **optimized-video-voice**| **optimized-voice**| **svp-voice**| **wmm-default**}

no ap dot11 {**24ghz**| **5ghz**} **edca-parameters** {**custom-voice**| **optimized-video-voice**| **optimized-voice**| **svp-voice**| **wmm-default**}

Syntax Description

24ghz	Specifies the 2.4 GHz band.
5ghz	Specifies the 5 GHz band.
edca-parameters	Specifies a specific enhanced distributed channel access (EDCA) profile on the 802.11 networks.
custom-voice	Enables custom voice EDCA parameters.
optimized-video-voice	Enables EDCA voice- and video-optimized profile parameters. Choose this option when both voice and video services are deployed on your network.
optimized-voice	Enables EDCA voice-optimized profile parameters. Choose this option when voice services other than SpectraLink are deployed on your network.
svp-voice	Enables SpectraLink voice priority parameters. Choose this option if SpectraLink phones are deployed on your network to improve the quality of calls.
wmm-default	Enables the Wi-Fi Multimedia (WMM) default parameters. Choose this option when voice or video services are not deployed on your network.

Command Default

wmm-default

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples This example shows how to enable SpectraLink voice priority parameters:

```
Controller(config)# ap dot11 24ghz edca-parameters svp-voice
```

ap dot11 rrm group-mode

To set the 802.11 automatic RF group selection mode on, use the **ap dot11 rrm group-mode** command. To set the 802.11 automatic RF group selection mode off, use the **no** form of this command.

ap dot11 {**5ghz**| **24ghz**} **rrm group-mode** {**auto**| **leader**| **off**| **restart**}

no ap dot11 {**5ghz**| **24ghz**} **rrm group-mode**

Syntax Description

5ghz	Specifies the 2.4 GHz band.
24ghz	Specifies the 5 GHz band.
auto	Sets the 802.11 RF group selection to automatic update mode.
leader	Sets the 802.11 RF group selection to static mode, and sets this controller as the group leader.
off	Sets the 802.11 RF group selection to off.
restart	Restarts the 802.11 RF group selection.

Command Default

auto

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to turn the auto RF group selection mode on the 5 GHz band:

```
Controller(config)# ap dot11 5ghz rrm group-mode auto
```

ap dot11 rrm channel cleanair-event

To configure CleanAir event-driven Radio Resource Management (RRM) parameters for all 802.11 Cisco lightweight access points, use the **ap dot11 rrm channel cleanair-event** command. When this parameter is configured, CleanAir access points can change their channel when a source of interference degrades the operations, even if the RRM interval has not expired yet.

ap dot11 {**24ghz**| **5ghz**} **rrm channel** {**cleanair-event sensitivity** *value*}

Syntax Description

24ghz	Specifies the 2.4 GHz band.
5ghz	Specifies the 5 GHz band.
sensitivity	Sets the sensitivity for CleanAir event-driven RRM.
value	Sensitivity value. You can specify any one of the following three optional sensitivity values: • **low—**Specifies low sensitivity. • **medium—**Specifies medium sensitivity. • **high—**Specifies high sensitivity.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to set the high sensitivity for CleanAir event-driven RRM:

```
Controller(config)# ap dot11 24ghz rrm channel cleanair-event sensitivity high
```

ap dot11 l2roam rf-params

To configure the 2.4 GHz or 5 GHz Layer 2 client roaming parameters, use the **ap dot11 l2roam rf-params** command.

ap dot11 {**24ghz**| **5ghz**} **l2roam rf-params custom** *min-rssi roam-hyst scan-thresh trans-time*

Syntax Description

24ghz	Specifies the 2.4 GHz band.
5ghz	Specifies the 5 GHz band.
custom	Specifies custom Layer 2 client roaming RF parameters.
min-rssi	Minimum received signal strength indicator (RSSI) that is required for the client to associate to the access point. If the client's average received signal power dips below this threshold, reliable communication is usually impossible. Clients must already have found and roamed to another access point with a stronger signal before the minimum RSSI value is reached. The valid range is –80 to –90 dBm, and the default value is –85 dBm.
roam-hyst	How much greater the signal strength of a neighboring access point must be in order for the client to roam to it. This parameter is intended to reduce the amount of roaming between access points if the client is physically located on or near the border between the two access points. The valid range is 2 to 4 dB, and the default value is 2 dB.
scan-thresh	Minimum RSSI that is allowed before the client should roam to a better access point. When the RSSI drops below the specified value, the client must be able to roam to a better access point within the specified transition time. This parameter also provides a power-save method to minimize the time that the client spends in active or passive scanning. For example, the client can scan slowly when the RSSI is above the threshold and scan more rapidly when the RSSI is below the threshold. The valid range is –70 to –77 dBm, and the default value is –72 dBm.
trans-time	Maximum time allowed for the client to detect a suitable neighboring access point to roam to and to complete the roam, whenever the RSSI from the client's associated access point is below the scan threshold. The valid range is 1 to 10 seconds, and the default value is 5 seconds.

Command Default

min-rssi	-85
roam-hyst	2
scan-thresh	-72
trans-time	5

Command Modes Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples This example shows how to configure custom Layer 2 client roaming parameters on an 802.11a network:

```
Controller(config)# ap dot11 5ghz l2roam rf-params custom -80 2 -70 7
```

ap dot11 media-stream

To configure media stream multicast-direct and video-direct settings on an 802.11 network, use the **ap dot11 media-stream** command.

ap dot11 {**24ghz**| **5ghz**} **media-stream** {**multicast-direct** {**admission-besteffort**| **client-maximum** *value*| **radio-maximum** *value*}| **video-redirect**}

Syntax Description

24ghz	Specifies the 2.4 GHz band.
5ghz	Specifies the 5 GHz band.
multicast-direct	Specifies the multicast-direct for the 2.4 GHz or a 5 GHz band.
admission-besteffort	Admits the media stream to the best-effort queue.
client-maximum *value*	Specifies the maximum number of streams allowed on a client.
radio-maximum *value*	Specifies the maximum number of streams allowed on a 2.4 GHz or a 5 GHz band.
video-redirect	Specifies the media stream video-redirect for the 2.4 GHz or a 5 GHz band.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Before you configure the media stream multicast-direct or video-redirect on a 802.11 network, ensure that the network is nonoperational.

Examples

This example shows how to enable media stream multicast-direct settings on the 5 GHz band:

```
Controller(config)# ap dot11 5ghz media-stream multicast-direct
```

This example shows how to admit the media stream to the best-effort queue if there is not enough bandwidth to prioritize the flow:

```
Controller(config)# ap dot11 5ghz media-stream multicast-direct admission-besteffort
```

This example shows how to set the maximum number of streams allowed on a client:

```
Controller(config)# ap dot11 5ghz media-stream multicast-direct client-maximum 10
```

This example shows how to enable media stream traffic redirection on the 5 GHz band:

```
Controller(config)# ap dot11 5ghz media-stream video-redirect
```

ap dot11 rrm ccx location-measurement

To configure cisco client Extensions (CCX) client location measurements for 2.4 GHz and 5 GHz bands, use the **ap dot11 rrm ccx location-measurement** command.

ap dot11 {**24ghz**| **5ghz**} **rrm ccx location-measurement** {**disable**| *interval*}

Syntax Description

24ghz	Specifies the 2.4-GHz band.
5ghz	Specifies the 5-GHz band.
disable	Disables support for CCX client location measurements.
interval	Interval from 10 to 32400.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to disable support for 2.4 GHz CCX client location measurements:

```
Controller(config)# no ap dot11 24ghz rrm ccx location-measurement
```

ap dot11 rrm channel dca

To configure Dynamic Channel Assignment (DCA) algorithm parameters on 802.11 networks, use the **ap dot11 rrm channel dca** command.

ap dot11 {**24ghz**| **5ghz**} **rrm channel dca**{*channel_number*| **anchor-time** *value*| **global**{**auto**| **once**}| **interval** *value*| **min-metric** *value*| **sensitivity**{**high**| **low**| **medium**}}

Syntax Description

24ghz	Specifies the 2.4 GHz band.
5ghz	Specifies the 5 GHz band.
channel_number	Channel number to be added to the DCA list. **Note** The range is from 1 to 14.
anchor-time	Specifies the anchor time for DCA.
value	Hour of time between 0 and 23. These values represent the hour from 12:00 a.m. to 11:00 p.m.
global	Specifies the global DCA mode for the access points in the 802.11 networks.
auto	Enables auto-RF.
once	Enables one-time auto-RF.
interval	Specifies how often the DCA is allowed to run.
value	Interval between the times when DCA is allowed to run. Valid values are 0, 1, 2, 3, 4, 6, 8, 12, or 24 hours. 0 is 10 minutes (600 seconds). Default value is 0 (10 minutes).
min-metric	Specifies the DCA minimum RSSI energy metric.
value	Minimum RSSI energy metric value from –100 to –60.
sensitivity	Specifies how sensitive the DCA algorithm is to environmental changes (for example, signal, load, noise, and interference) when determining whether or not to change channels.
high	Specifies that the DCA algorithm is not particularly sensitive to environmental changes. See the “Usage Guidelines” section for more information.
low	Specifies that the DCA algorithm is moderately sensitive to environmental changes. See the “Usage Guidelines” section for more information.
medium	Specifies that the DCA algorithm is highly sensitive to environmental changes. See the “Usage Guidelines” section for more information.

Command Default None

Command Modes Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines The DCA sensitivity thresholds vary by radio band as shown in the table below.

To aid in troubleshooting, the output of this command shows an error code for any failed calls. The table below explains the possible error codes for failed calls.

Table 20: DCA Sensitivity Threshold

Sensitivity	2.4 Ghz DCA Sensitivity Threshold	5 Ghz DCA Sensitivity Threshold
High	5 dB	5 dB
Medium	15 dB	20 dB
Low	30 dB	35 dB

Examples This example shows how to configure the controller to start running DCA at 5 pm for the 2.4 GHz band:

```
Controller(config)# ap dot11 24ghz rrm channel dca anchor-time 17
```

This example shows how to set the DCA algorithm to run every 10 minutes for the 2.4 GHz band:

```
Controller(config)# ap dot11 24ghz rrm channel dca interval 0
```

This example shows how to configure the value of DCA algorithm's sensitivity to low on the 2.4 GHz band:

```
Controller(config)# ap dot11 24ghz rrm channel dca sensitivity low
```

ap dot11 rrm group-member

To configure members in an 802.11 static RF group, use the **ap dot11 rrm group-member** command. To remove members from 802.11 RF group, use the **no** form of this command.

ap dot11 {**24ghz**| **5ghz**} **rrm group-member** *controller-name controller-ip*

no ap dot11 {**24ghz**| **5ghz**} **rrm group-member** *controller-name controller-ip*

Syntax Description

24ghz	Specifies the 2.4 GHz band.
5ghz	Specifies the 5 GHz band.
controller-name	Name of the controller to be added.
controller-ip	IP address of the controller to be added.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to add a controller in the 5 GHz band RF group:

```
Controller(config)# ap dot11 5ghz rrm group-member cisco-controller 192.0.2.54
```

ap dot11 rrm logging

To configure report log settings on supported 802.11 networks, use the **ap dot11 rrm logging** command.

ap dot11 {**24ghz**| **5ghz**} **rrm logging** {**channel**| **coverage**| **foreign**| **load**| **noise**| **performance**| **txpower**}

Syntax Description

24ghz	Specifies the 2.4 GHz band.
5ghz	Specifies the 5 GHz band.
channel	Turns the channel change logging mode on or off. The default mode is off (Disabled).
coverage	Turns the coverage profile logging mode on or off. The default mode is off (Disabled).
foreign	Turns the foreign interference profile logging mode on or off. The default mode is off (Disabled).
load	Turns the load profile logging mode on or off. The default mode is off (Disabled).
noise	Turns the noise profile logging mode on or off. The default mode is off (Disabled).
performance	Turns the performance profile logging mode on or off. The default mode is off (Disabled).
txpower	Turns the transit power change logging mode on or off. The default mode is off (Disabled).

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to turn the 5 GHz logging channel selection mode on:

```
Controller(config)# ap dot11 5ghz rrm logging channel
```

This example shows how to turn the 5 GHz coverage profile violation logging selection mode on:

```
Controller(config)# ap dot11 5ghz rrm logging coverage
```

This example shows how to turn the 5 GHz foreign interference profile violation logging selection mode on:

```
Controller(config)# ap dot11 5ghz rrm logging foreign
```

This example shows how to turn the 5 GHz load profile logging mode on:

```
Controller(config)# ap dot11 5ghz rrm logging load
```

This example shows how to turn the 5 GHz noise profile logging mode on:

```
Controller(config)# ap dot11 5ghz rrm logging noise
```

This example shows how to turn the 5 GHz performance profile logging mode on:

```
Controller(config)# ap dot11 5ghz rrm logging performance
```

This example shows how to turn the 5 GHz transmit power change mode on:

```
Controller(config)# ap dot11 5ghz rrm logging txpower
```

ap dot11 rrm monitor

To Configure monitor settings on the 802.11 networks, use the **ap dot11 rrm monitor** command.

ap dot11 {**24ghz**| **5ghz**} **rrm monitor**{**channel-list**| {**all**| **country**| **dca**}| **coverage**| **load**| **noise**| **signal**} *seconds*

Syntax Description

24ghz	Specifies the 802.11b parameters.
5ghz	Specifies the 802.11a parameters.
channel-list all	Monitors the noise, interference, and rogue monitoring channel list for all channels.
channel-list country	Monitors the noise, interference, and rogue monitoring channel list for the channels used in the configured country code.
channel-list dca	Monitors the noise, interference, and rogue monitoring channel list for the channels used by automatic channel assignment.
coverage	Specifies the coverage measurement interval.
load	Specifies the load measurement interval.
noise	Specifies the noise measurement interval.
signal	Specifies the signal measurement interval.
seconds	Measurement interval time from 60 to 3600 seconds.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to monitor the channels used in the configured country:

```
Controller(config)# ap dot11 24ghz rrm monitor channel-list country
```

This example shows how to set the coverage measurement interval to 60 seconds:

```
Controller(config)# ap dot11 24ghz rrm monitor coverage 60
```

ap dot11 rrm ndp-type

To configure the 802.11 access point radio resource management neighbor discovery protocol type, use the **ap dot11 rrm ndp-type** command.

ap dot11 {**24ghz**| **5ghz**} **rrm ndp-type** {**protected**| **transparent**}

Syntax Description

24ghz	Specifies the 2.4 GHz band.
5ghz	Specifies the 5 GHz band.
protected	Specifies the Tx RRM protected (encrypted) neighbor discovery protocol.
transparent	Specifies the Tx RRM transparent (not encrypted) neighbor discovery protocol.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Before you configure the 802.11 access point RRM neighbor discovery protocol type, ensure that you have disabled the network by entering the **ap dot11** {**24ghz | 5ghz**} **shutdown** command.

Examples

This example shows how to enable the 802.11a access point RRM neighbor discovery protocol type as protected:

```
Controller(config)# ap dot11 5ghz rrm ndp-type protected
```

ap dot1x max-sessions

To configure the maximum number of simultaneous 802.1X sessions allowed per access point, use the **ap dot1x max-sessions** command.

ap dot1x max-sessions *num-of-sessions*

Syntax Description

num-of-sessions	Number of maximum 802.1X sessions initiated per AP at a time. The range is from 0 to 255, where 0 indicates unlimited.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

It is required to limit the number of simultaneous 802.1X sessions initiated per access point to protect against flooding attacks caused by using 802.1X messages.

Examples

This example shows how to configure the maximum number of simultaneous 802.1X sessions:

```
Controller(config)# ap dot1x max-sessions 100
```

ap dot1x username

To configure the 802.1X username and password for all access points that are currently joined to the controller and any access points that join the controller in the future, use the **ap dot1x username** command. To disable the 802.1X username and password for all access points that are currently joined to the controller, use the **no** form of this command.

ap dot1x username *user-id* **password** {**0**| **8**} *password-string*

no ap dot1x username *user-id***password** {**0**| **8**} *password-string*

Syntax Description

user-id	Username.
password	Specifies an 802.1X password for all access points.
0	Specifies an unencrypted password.
8	Specifies an AES encrypted password.
password_string	Password.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You should enter a strong password. Strong passwords have the following characteristics:

- They are at least eight characters long.
- They contain a combination of uppercase and lowercase letters, numbers, and symbols.
- They are not words in any language.

You can set the values for a specific access point.

Examples

This example shows how to configure the global authentication username and password for all access points:

```
Controller(config)# ap dot1x username cisco123 password 0 cisco2020
```

ap ethernet duplex

To configure the Ethernet port duplex and speed settings of the lightweight access points, use the **ap ethernet duplex** command. To disable the Ethernet port duplex and speed settings of lightweight access points, use the **no** form of this command.

ap ethernet duplex *duplex* **speed** *speed*

no ap ethernet

Syntax Description

duplex	Ethernet port duplex settings. You can specify the following options to configure the duplex settings: • **auto—**Specifies the Ethernet port duplex auto settings. • **half—**Specifies the Ethernet port duplex half settings. • **full—**Specifies the Ethernet port duplex full settings.
speed	Specifies the Ethernet port speed settings.
speed	Ethernet port speed settings. You can specify the following options to configure the speed settings: • **auto—**Specifies the Ethernet port speed to auto. • **10—**Specifies the Ethernet port speed to 10 Mbps. • **100—**Specifies the Ethernet port speed to 100 Mbps. • **1000—**Specifies the Ethernet port speed to 1000 Mbps.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to configure the Ethernet port duplex full settings as 1000 Mbps for all access points:

```
Controller(config)# ap ethernet duplex full speed 1000
```

ap group

To create a new access point group, use the **ap group** command. To remove an access point group, use the **no** form of this command.

ap group *group-name*

no ap group *group-name*

Syntax Description

group-name	Access point group name.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

An error message appears if you try to delete an access point group that is used by at least one access point. Before you can delete an AP group, move all APs in this group to another group. The access points are not moved to the default-group access point group automatically. To see the APs, enter the **show ap summary** command. To move access points, enter the **ap name** *Cisco-AP* **ap-groupname** *Group-Name* command.

Examples

This example shows how to create a new access point group:

```
Controller(config)# ap group sampleapgroup
```

ap image

To configure an image on all access points that are associated to the controller, use the **ap image** command.

ap image {**predownload**| **reset**| **swap**}

Syntax Description

predownload	Instructs all the access points to start predownloading an image.
reset	Instructs all the access points to reboot.
swap	Instructs all the access points to swap the image.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to predownload an image to all access points:

```
Controller# ap image predownload
```

This example shows how to reboot all access points:

```
Controller# ap image reset
```

This example shows how to swap the access point's primary and secondary images:

```
Controller# ap image swap
```

ap led

To enable the LED state for an access point, use the **ap led** command. To disable the LED state for an access point, use the **no** form of this command.

ap led

no ap led

Syntax Description

This command has no keywords and arguments.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to enable the LED state for an access point:

```
Controller(config)# ap led
```

ap link-encryption

To enable Datagram Transport Layer Security (DTLS) data encryption for access points, use the **ap link-encryption** command. To disable the DTLS data encryption for access points, use the **no** form of this command.

ap link-encryption

no ap link-encryption

Syntax Description

This command has no keywords and arguments.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to enable data encryption for all the access points that are joined to the controller:

```
Controller(config)# ap link-encryption
```

ap link-latency

To enable link latency for all access points that are currently associated to the controller, use the **ap link-latency** command. To disable link latency all access points that are currently associated to the controller, use the **no** form of this command.

ap link-latency [**reset**]

no ap link-latency

Syntax Description

reset	(Optional) Resets all link latency for all access points.

Command Default

Link latency is disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

This command enables or disables link latency only for those access points that are currently joined to the controller. It does not apply to access points that join in the future.

Examples

This example shows how to enable the link latency for all access points:

```
Controller(config)# ap link-latency
```

ap mgmtuser username

To configure the username, password, and secret password for access point management, use the **ap mgmtuser username** command.

ap mgmtuser username *username* **password** *password_type password* **secret** *secret_type secret*

Syntax Description

username	Specifies the username for access point management.
password	Specifies the password for access point management.
password_type	Password type. You can specify any one of the following two password types: • **0**—Specifies that an unencrypted password will follow. • **8**—Specifies that an AES encrypted password will follow.
password	Access point management password.
secret	Specifies the secret password for privileged access point management.
secret_type	Secret type. You can specify any one of the following two secret types: • **0**—Specifies that an unencrypted secret password will follow. • **8**—Specifies that an AES encrypted secret password will follow.
secret	Access point management secret password.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

To specify a strong password, the following password requirements should be met:

- The password should contain characters from at least three of the following classes: lowercase letters, uppercase letters, digits, and special characters.
- No character in the password can be repeated more than three times consecutively.
- The password should not contain a management username or the reverse of a username.
- The password should not contain words such as Cisco, oscic, admin, nimda or any variant obtained by changing the capitalization of letters by substituting 1, |, or ! or substituting 0 for o or substituting $ for s.

To specify a strong secret password, the following requirement should be met:

- The secret password should contain characters from at least three of the following classes: lowercase letters, uppercase letters, digits, or special characters.

Examples

This example shows how to add a username, password, and secret password for access point management:

```
Controller(config)# ap mgmtuser username glbusr password 0 Arc_1234 secret 0 Mid_1234
```

ap name ap-groupname

To add a Cisco lightweight access point to a specific access point group, use the **ap name ap-groupname** command.

ap name *ap-name* **ap-groupname** *group-name*

Syntax Description

ap-name	Name of the Cisco lightweight access point.
group-name	Descriptive name for the access point group.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The Cisco lightweight access point must be disabled before changing this parameter.

Examples

This example shows how to add the access point AP01 to the access point group superusers:

```
Controller# ap name AP01 ap-groupname superusers
```

ap name bhrate

To configure the Cisco bridge backhaul Tx rate, use the **ap name bhrate** command.

ap name *ap-name* **bhrate** *kbps*

Syntax Description

ap-name	Name of the Cisco access point.
kbps	Cisco bridge backhaul Tx rate in kbps. The valid values are 6000, 12000, 18000, 24000, 36000, 48000, and 54000.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to configure the Cisco bridge backhaul Tx rate to 54000 kbps:

```
Controller# ap name AP02 bhrate 54000
```

ap name bridgegroupname

To set a bridge group name on a Cisco lightweight access point, use the **ap name bridgegroupname** command. To delete a bridge group name on a Cisco lightweight access point, use the **no** form of this command.

ap name *ap-name* **bridgegroupname** *bridge_group_name*

ap name *ap-name* **no bridgegroupname**

Syntax Description

ap-name	Name of the Cisco lightweight access point.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Only access points with the same bridge group name can connect to each other. Changing the access point bridgegroupname may strand the bridge access point.

Examples

This example shows how to set a bridge group name on Cisco access point's bridge group name AP02:

```
Controller# ap name AP02 bridgegroupname West
```

This example shows how to delete a bridge group name on Cisco access point's bridge group name AP02:

```
Controller# ap name AP02 no bridgegroupname
```

ap name capwap retransmit

To configure the access point control packet retransmission interval and control packet retransmission count, use the **ap name capwap retransmit** command.

ap name *ap-name* **capwap retransmit** {**count** *count-value*| **interval** *interval-time*}

Syntax Description

ap-name	Name of the Cisco lightweight access point.
count	Sets the number of times control packet will be retransmitted.
count-value	Number of times that the control packet will be retransmitted from 3 to 8.
interval	Sets the control packet retransmission timeout interval.
interval-time	Control packet retransmission timeout from 2 to 5 seconds.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to configure the retransmission interval for an access point:

```
Controller# ap name AP01 capwap retransmit interval 5
```

This example shows how to configure the retransmission retry count for a specific access point:

```
Controller# ap name AP01 capwap retransmit count 5
```

ap name command

To execute a command remotely on a specific Cisco access point, use the **ap name command** command.

ap name *ap-name* **command** *command*

Syntax Description

ap-name	Name of the Cisco access point.
command	Command to be executed on a Cisco access point.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to remotely enter the **show ip interface brief** command on the Cisco access point named TSIM_AP2:

```
Controller# ap name AP2 command show ip interface brief
```

ap name core-dump

To configure a Cisco lightweight access point's memory core dump, use the **ap name core-dump** command. To disable a Cisco lightweight access point's memory core dump, use the **no** form of this command.

ap name *ap-name* **core-dump** *tftp-ip-addr filename* {**compress**| **uncompress**}

ap name *ap-name* [**no**]**core-dump**

Syntax Description

ap-name	Name of the access point.
tftp-ip-addr	IP address of the TFTP server to which the access point sends core dump files.
filename	Name that the access point used to label the core file.
compress	Compresses the core dump file.
uncompress	Uncompresses the core dump file.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The access point must be able to reach the TFTP server before you can use this command.

Examples

This example shows how to configure and compress the core dump file:

```
Controller# ap name AP2 core-dump 192.1.1.1 log compress
```

ap name country

To configure the country of operation for a Cisco lightweight access point, use the **ap name country** command.

ap name *ap-name* **country** *country-code*

Syntax Description

ap-name	Name of the Cisco lightweight access point.
country-code	Two-letter or three-letter country code.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Cisco controllers must be installed by a network administrator or qualified IT professional and the installer must select the proper country code. Following installation, access to the unit should be password protected by the installer to maintain compliance with regulatory requirements and to ensure proper unit functionality. See the related product guide for the most recent country codes and regulatory domains. Also, access point regulatory domains are defined during the access point manufacturing process. You can change the access point country code if the new country code matches a country that is valid within the access point regulatory domain. If you try to enter a country that is not valid to the access point regulatory domain, the command fails.

Examples

This example shows how to configure the Cisco lightweight access point's country code to DE:

```
Controller# ap name AP2 country JP
```

ap name crash-file

To manage crash data and radio core files for the Cisco access point, use the **ap name crash-file** command.

ap name *ap-name* **crash-file** {**get-crash-data**| **get-radio-core-dump** {**slot 0**| **slot 1**}}

Syntax Description

ap-name	Name of the Cisco lightweight access point.
get-crash-data	Collects the latest crash data for a Cisco lightweight access point.
get-radio-core-dump	Gets a Cisco lightweight access point's radio core dump
slot	Slot ID for Cisco access point.
0	Specifies Slot 0.
1	Specifies Slot 1.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to collect the latest crash data for access point AP3:

```
Controller# ap name AP3 crash-file get-crash-data
```

This example shows how to collect the radio core dump for access point AP02 and slot 0:

```
Controller# ap name AP02 crash-file get-radio-core-dump slot 0
```

ap name dot11 24ghz rrm coverage

To configure coverage hole detection settings on the 2.4 GHz band, use the **ap name dot11 24ghz rrm coverage** command.

ap name *ap-name* **dot11 24ghz rrm coverage** {**exception** *value*| **level** *value*}

Syntax Description

ap-name	Name of the Cisco access point.
exception	Specifies the percentage of clients on an access point that are experiencing a low signal level but cannot roam to another access point.
value	Percentage of clients. Valid values are from 0 to 100%. **Note** The default is 25%.
level	Specifies the minimum number of clients on an access point with a received signal strength indication (RSSI) value at or below the data or voice RSSI threshold.
value	Minimum number of clients. Valid values are from 1 to 75. **Note** The default is 3.

Command Default

The default for the *exception* parameter is 25% and the default for the *level* parameter is 3.

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

If you enable coverage hole detection, the controller automatically determines, based on data that is received from the access points, whether any access points have clients that are potentially located in areas with poor coverage.

If both the number and percentage of failed packets exceed the values that you entered in the **ap dot11 24ghz rrm coverage data packet-count** *count* and **ap dot11 24ghz rrm coverage data fail-percentage** *percentage* commands for a 5-second period, the client is considered to be in a pre-alarm condition. The controller uses this information to distinguish between real and false coverage holes and excludes clients with poor roaming logic. A coverage hole is detected if both the number and percentage of failed clients meet or exceed the values entered in the **ap dot11 24ghz rrm coverage exception** and **ap dot11 24ghz rrm coverage level** commands over a 90-second period. The controller determines whether the coverage hole can be corrected

and, if appropriate, mitigates the coverage hole by increasing the transmit power level for that specific access point.

Examples

This example shows how to specify the percentage of clients for an access point 2.4 GHz radio that is experiencing a low signal level:

```
Controller# ap name AP2 dot11 24ghz rrm coverage exception 25%
```

This example shows how to specify the minimum number of clients on an 802.11b access point with an RSSI value at or below the RSSI threshold:

```
Controller# ap name AP2 dot11 24ghz rrm coverage level 60
```

ap name dot11 49ghz rrm profile

To configure Radio Resource Management (RRM) performance profile settings for a Cisco lightweight access point on a 4.9 GHz public safety channel, use the **ap name dot11 49ghz rrm profile** command.

ap name *ap-name* **dot11 49ghz rrm profile** {**clients** *value*| **customize**| **exception** *value*| **foreign** *value*| **level** *value*| **noise** *value*| **throughput** *vaue*| **utilization** *value*}

Syntax Description

ap-name	Name of the Cisco lightweight access point.
clients	Sets the access point client threshold.
value	Access point client threshold from 1 to 75 clients. **Note** The default client threshold is 12.
customize	Turns on performance profile customization for an access point. **Note** Performance profile customization is off by default.
exception *value*	Sets the 802.11a Cisco access point coverage exception level from 0 to100 percent.
foreign	Sets the foreign 802.11 transmitter interference threshold.
value	Foreign 802.11 transmitter interference threshold from 0 to 100 percent. **Note** The default is 10 percent.
level *value*	Sets the 802.11a Cisco access point client minimum exception level from 1 to 75 clients.
noise	Sets the 802.11 foreign noise threshold.
value	802.11 foreign noise threshold from –127 to 0 dBm. **Note** The default is –70 dBm.
throughput	Sets the data-rate throughput threshold.
value	802.11 throughput threshold from 1000 to 10000000 bytes per second. **Note** The default is 1,000,000 bytes per second.
utilization	Sets the RF utilization threshold. **Note** The operating system generates a trap when this threshold is exceeded.

value	802.11 RF utilization threshold from 0 to 100 percent. **Note** The default is 80 percent.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to set the AP1 clients threshold to 75 clients:

```
Controller# ap name AP1 dot11 49ghz rrm profile clients 75
```

This example shows how to turn performance on profile customization for Cisco lightweight access point AP1 on the 4.9 GHz channel:

```
Controller# ap name AP1 dot11 49ghz rrm profile customize
```

This example shows how to set the foreign transmitter interference threshold for AP1 to 0 percent:

```
Controller# ap name AP1 dot11 49ghz rrm profile foreign 0
```

This example shows how to set the foreign noise threshold for AP1 to 0 dBm:

```
Controller# ap name AP1 dot11 49ghz rrm profile noise 0
```

This example shows how to set the AP1 data-rate threshold to 10000000 bytes per second:

```
Controller# ap name AP1 dot11 49ghz rrm profile throughput 10000000
```

This example shows how to set the RF utilization threshold for AP1 to 100 percent:

```
Controller# ap name AP1 dot11 49ghz rrm profile utilization 100
```

ap name dot11 5ghz rrm channel

To configure a new channel using an 802.11h channel announcement, use the **ap name dot11 5ghz rrm channel** command.

ap name *ap-name* **dot11 5ghz rrm channel** *channel*

Syntax Description

ap-name	Name of the Cisco lightweight access point.
channel	New channel.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to configure a new channel using the 802.11h channel:

```
Controller# ap name AP01 dot11 5ghz rrm channel 140
```

ap name dot11 antenna

To configure radio antenna settings for Cisco lightweight access points on different 802.11 networks, use the **ap name dot11 antenna** command.

ap name *ap-name* **dot11** {**24ghz**| **5ghz**} **antenna** {**ext-ant-gain** *gain*| **mode** {**omni**| **sectorA**| **sectorB**}| **selection** {**external**| **internal**}}

Syntax Description

ap-name	Name of the Cisco lightweight access point.
24ghz	Specifies the 2.4 GHz band.
5ghz	Specifies the 5 GHz band.
ext-ant-gain	Specifies the external antenna gain for an 802.11 network. **Note** Before you enter this command, disable the Cisco radio by using the **ap dot11** {**24ghz** | **5ghz**} **shutdown** command. After you enter this command, reenable the Cisco radio by using the **no ap dot11** {**24ghz** | **5ghz**} **shutdown** command.
gain	Antenna gain in 0.5 dBm units (for example, 2.5 dBm = 5).
mode	Specifies that the Cisco lightweight access point is to use one internal antenna for an 802.11 sectorized 180-degree coverage pattern or both internal antennas for an 802.11 360-degree omnidirectional pattern.
omni	Specifies to use both internal antennas.
sectorA	Specifies to use only the side A internal antenna.
sectorB	Specifies to use only the side B internal antenna.
selection	Selects the internal or external antenna selection for a Cisco lightweight access point on an 802.11 network.
external	Specifies the external antenna.
internal	Specifies the internal antenna.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to configure a 5 GHz external antenna gain of 0.5 dBm for AP1:

```
Controller# ap name AP1 dot11 5ghz antenna ext-ant-gain 0.5
```

This example shows how to configure access point AP01 antennas for a 360-degree omnidirectional pattern on a 2.4 GHz band:

```
Controller# ap name AP01 dot11 24ghz antenna mode omni
```

This example shows how to configure access point AP02 on a 2.4 GHz band to use the internal antenna:

```
Controller# ap name AP02 dot11 24ghz antenna selection interval
```

ap name dot11 antenna extantgain

To configure radio antenna settings for Cisco lightweight access points on 4.9 GHz and 5.8 GHz public safety channels, use the **ap name dot11 antenna extantgain** command.

ap name *ap-name* **dot11** {**49ghz**| **58ghz**} {**antenna extantgain** *gain*}

Syntax Description

ap-name	Name of the Cisco lightweight access point.
49ghz	Specifies 4.9 GHz public safety channel settings.
58ghz	Specifies 5.8 GHz public safety channel settings.
gain	Antenna gain in 0.5 dBm units (for example, 2.5 dBm = 5).

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Before you enter this command, disable the Cisco radio by using the **ap dot11** {**24ghz | 5ghz**} **shutdown** command. After you enter this command, reenable the Cisco radio by using the **no ap dot11** {**24ghz | 5ghz**} **shutdown** command.

Examples

This example shows how to configure an external antenna gain of 0.5 dBm for AP1 on a 4.9 GHz public safety channel:

```
Controller# ap name AP1 dot11 49ghz antenna extantgain 0.5
```

ap name dot11 cleanair

To configure CleanAir settings for a specific Cisco lightweight access point on 802.11 networks, use the **ap name dot11 cleanair** command.

ap name *ap-name* **dot11** {**24ghz**| **5ghz**} **cleanair**

Syntax Description

ap-name	Name of the Cisco lightweight access point.
24ghz	Specifies the 2.4 GHz band.
5ghz	Specifies the 5 GHz band.

Command Default

Disabled.

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to enable CleanAir on the 2.4 GHz band:

```
Controller# ap name AP01 dot11 24ghz cleanair
```

ap name dot11 dot11n antenna

To configure an access point to use a specific antenna, use the **ap name dot11 dot11n antenna** command.

ap name *ap-name* **dot11** {**24ghz**| **5ghz**} **dot11n antenna** {**A**| **B**| **C**| **D**}

Syntax Description

ap-name	Access point name.
24ghz	Specifies the 2.4 GHz band.
5ghz	Specifies the 5 GHz band.
A	Specifies antenna port A.
B	Specifies antenna port B.
C	Specifies antenna port C.
D	Specifies antenna port D.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to enable antenna B on access point AP02:

```
Controller# ap name AP02 dot11 5ghz dot11n antenna B
```

This example shows how to disable antenna C on access point AP02:

```
Controller# ap name AP02 no dot11 5ghz dot11n C
```

ap name dot11 rrm ccx

To configure Cisco Client eXtension (CCX) Radio Resource Management (RRM) settings for specific Cisco lightweight access points on 802.11 networks, use the **ap name dot11 rrm ccx** command.

ap name *ap-name* **dot11** {**24ghz**| **5ghz**} **rrm ccx** {**customize**| **location-measurement** *interval*}

Syntax Description

ap-name	Name of the Cisco lightweight access point.
24ghz	Specifies the 2.4 GHz band.
5ghz	Specifies the 5 GHz band.
customize	Enables 802.11 CCX options.
location-measurement	Configures the CCX client location measurements.
interval	Interval from 10 to 32400.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to configure CCX client location measurements for an access point in the 2.4 GHz band:

```
Controller# ap name AP01 dot11 24ghz rrm ccx location-measurement 3200
```

ap name dot11 rrm profile

To configure Radio Resource Management (RRM) performance profile settings for a Cisco lightweight access point, use the **ap name dot11 rrm profile** command.

ap name *ap-name* **dot11** {**24ghz**| **5ghz**} **rrm profile** {**clients** *value*| **customize**| **foreign** *value*| **noise** *value*| **throughput** *value*| **utilization** *value*}

Syntax Description

ap-name	Name of the Cisco lightweight access point.
24ghz	Specifies the 2.4 GHz band.
5ghz	Specifies the 5 GHz band.
clients	Sets the access point client threshold.
value	Access point client threshold from 1 to 75 clients. **Note** The default client threshold is 12.
customize	Turns on performance profile customization for an access point. **Note** Performance profile customization is off by default.
foreign	Sets the foreign 802.11 transmitter interference threshold.
value	Foreign 802.11 transmitter interference threshold from 0 to 100 percent. **Note** The default is 10 percent.
noise	Sets the 802.11 foreign noise threshold.
value	802.11 foreign noise threshold between –127 and 0 dBm. **Note** The default is —70 dBm.
throughput	Sets the data-rate throughput threshold.
value	802.11 throughput threshold from 1000 to 10000000 bytes per second. **Note** The default is 1,000,000 bytes per second.
utilization	Sets the RF utilization threshold. **Note** The operating system generates a trap when this threshold is exceeded.
value	802.11 RF utilization threshold from 0 to 100 percent. **Note** The default is 80 percent.

Command Default None

Command Modes Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to set the AP1 clients threshold to 75 clients:

```
Controller# ap name AP1 dot11 24ghz rrm profile clients 75
```

This example shows how to turn performance profile customization on for 802.11a Cisco lightweight access point AP1:

```
Controller# ap name AP1 dot11 5ghz rrm profile customize
```

This example shows how to set the foreign 802.11a transmitter interference threshold for AP1 to 0 percent:

```
Controller# ap name AP1 dot11 5ghz rrm profile foreign 0
```

This example shows how to set the 802.11a foreign noise threshold for AP1 to 0 dBm:

```
Controller# ap name AP1 dot11 5ghz rrm profile noise 0
```

This example shows how to set the AP1 data-rate threshold to 10000000 bytes per second:

```
Controller# ap name AP1 dot11 5ghz rrm profile throughput 10000000
```

This example shows how to set the RF utilization threshold for AP1 to 100 percent:

```
Controller# ap name AP1 dot11 5ghz rrm profile utilization 100
```

ap name dot11 txpower

To configure the transmit power level for a single access point in an 802.11 network, use the **ap name dot11 txpower** command.

ap name *ap-name* **dot11** {**24ghz**| **5ghz**} {**shutdown**| **txpower** {**auto**| *power-level*}}

Syntax Description

ap-name	Name of the Cisco lightweight access point.
24ghz	Specifies the 2.4 GHz band.
5ghz	Specifies the 5 GHz band.
shutdown	Disables the 802.11 networks.
auto	Specifies the power level is automatically set by Radio Resource Management (RRM) for the 802.11 Cisco radio.
power-level	Manual transmit power level number for the access point.

Command Default

The command default (txpower auto) is for automatic configuration by RRM.

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to automatically set the 2.4 GHz radio transmit power for access point AP1:

```
Controller# ap name AP1 dot11 24ghz txpower auto
```

ap name dot1x-user

To configure the global authentication username and password for an access point that is currently joined to the controller, use the **ap name dot1x-user** command. To disable 802.1X authentication for a specific access point, use the **no** form of this command.

ap name *ap-name* **dot1x-user** {**global-override**| **username** *user-id* **password** *passwd*}

ap name *ap-name* [**no**] **dot1x-user**

Syntax Description

ap-name	Name of the access point.
global-override	Forces the access point to use the controller's global authentication settings.
username	Specifies to add a username.
user-id	Username.
password	Specifies to add a password.
passwd	Password.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You should enter a strong password. Strong passwords have the following characteristics:

- They are at least eight characters long.
- They contain a combination of uppercase and lowercase letters, numbers, and symbols.
- They are not words in any language.

  You can set the values for a specific access point.

You can disable 802.1X authentication for a specific access point only if global 802.1X authentication is not enabled. If global 802.1X authentication is enabled, you can disable 802.1X for all access points only.

Examples

This example shows how to configure a specific username and password for dot1x authentication:

```
Controller# ap name AP02 dot1x-user username Cisco123 password Cisco2020
```

This example shows how to disable the authentication for access point cisco_ap1:

```
Controller# ap name cisco_ap1 no dot1x-user
```

ap name ethernet

To configure ethernet port settings of a Cisco lightweight access point, use the **ap name ethernet** command. To remove configured port settings or set of defaults, use the **no** form of this command.

ap name *ap-name* **ethernet** *intf-number* **mode** {**access** *vlan-id*| **trunk** [**add**| **delete**]} **native-vlan** *vlan-id*

ap name *ap-name* **no ethernet** *intf-number* **mode** {**access**| **trunk native-vlan**}

Syntax Description

ap-name	Name of the Cisco lightweight access point.
intf-number	Ethernet interface number from 0 to 3.
mode	Configures access or trunk mode.
access	Configures the port in access mode.
vlan-id	VLAN identifier.
trunk	Specifies the port in trunk mode.
add	(Optional) Adds a VLAN or trunk mode.
delete	(Optional) Deletes a VLAN or trunk mode.
native-vlan	Specifies a native VLAN.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to configure access mode for a Cisco access point.

```
Controller# ap name AP2 ethernet 0 mode access 1
```

ap name ethernet duplex

To configure the Ethernet port duplex and speed settings of the lightweight access points, use the **ap name ethernet duplex** command.

ap name *ap-name* **ethernet duplex** {**auto**| **full**| **half**} **speed**{**10**| **100**| **1000**| **auto**}

Syntax Description

ap-name	Name of the Cisco access point.
auto	Specifies the Ethernet port duplex auto settings.
full	Specifies the Ethernet port duplex full settings.
half	Specifies the Ethernet port duplex half settings.
speed	Specifies the Ethernet port speed settings.
10	Specifies the Ethernet port speed to 10 Mbps.
100	Specifies the Ethernet port speed to 100 Mbps.
1000	Specifies the Ethernet port speed to 1000 Mbps.
auto	Specifies the Ethernet port setting for all connected access points.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to configure the Ethernet port to full duplex and 1 Gbps for an access point:

```
Controller# ap name AP2 ethernet duplex full 1000
```

ap name image

To configure an image on a specific access point, use the **ap name image** command.

ap name *ap-name* **image** {**predownload**| **swap**}

Syntax Description

ap-name	Name of the Cisco lightweight access point.
predownload	Instructs the access point to start the image predownload.
swap	Instructs the access point to swap the image.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to predownload an image to an access point:

```
Controller# ap name AP2 image predownload
```

This example shows how to swap an access point's primary and secondary images:

```
Controller# ap name AP2 image swap
```

ap name led

To enable the LED state for an access point, use the **ap name led** command. To disable the LED state for an access point, use the **no** form of this command.

ap name *ap-name* **led**

no ap name *ap-name* [**led**] **led**

Syntax Description

ap-name	Name of the Cisco lightweight access point.
led	Enables the access point's LED state.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to enable the LED state for an access point:

```
Controller# ap name AP2 led
```

This example shows how to disable the LED state for an access point:

```
Controller# ap name AP2 no led
```

ap name location

To modify the descriptive location of a Cisco lightweight access point, use the **ap name location** command.

ap name *ap-name* **location** *location*

Syntax Description

ap-name	Name of the Cisco lightweight access point.
location	Location name of the access point (enclosed by double quotation marks).

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The Cisco lightweight access point must be disabled before changing this parameter.

Examples

This example shows how to configure the descriptive location for access point AP1:

```
Controller# ap name AP1 location Building1
```

ap name mgmtuser

To configure the username, password, and secret password for access point management, use the **ap name mgmtuser** command. To force a specific access point to use the controller's global credentials, use the **no** form of this command.

ap name *ap-name* **mgmtuser username** *username* **password** *password* **secret** *secret*

ap name *ap-name* **no mgmtuser**

Syntax Description

ap-name	Name of the Cisco lightweight access point.
username	Specifies the username for access point management.
username	Management username.
password	Specifies the password for access point management.
password	Access point management password.
secret	Specifies the secret password for privileged access point management.
secret	Access point management secret password.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

To specify a strong password, you should adhere to the following requirements:

- The password should contain characters from at least three of the following classes: lowercase letters, uppercase letters, digits, and special characters.
- No character in the password can be repeated more than three times consecutively.
- The password cannot contain a management username or the reverse of a username.
- The password cannot contain words such as Cisco, oscic, admin, nimda or any variant obtained by changing the capitalization of letters by substituting 1, |, or ! or substituting 0 for o or substituting $ for s.

The following requirement is enforced on the secret password:

- The secret password cannot contain characters from at least three of the following classes: lowercase letters, uppercase letters, digits, or special characters.

Examples

This example shows how to add a username, password, and secret password for access point management:

```
Controller# ap name AP01 mgmtuser username acd password Arc_1234 secret Mid_1234
```

ap name mode

To change a Cisco controller communication option for an individual Cisco lightweight access point, use the **ap name mode** command.

ap name *ap-name* **mode**{**local submode**{**none**| **wips**}| **monitor submode**{**none**| **wips**}| **rogue**| **se-connect**| **sniffer**}

Syntax Description

ap-name	Name of the Cisco lightweight access point.
local	Converts from an indoor mesh access point (MAP or RAP) to a nonmesh lightweight access point (local mode).
submode	Specifies wIPS submode on an access point.
none	Disables the wIPS on an access point.
monitor	Specifies monitor mode settings.
wips	Enables the wIPS submode on an access point.
rogue	Enables wired rogue detector mode on an access point.
se-connect	Enables spectrum expert mode on an access point.
sniffer	Enables wireless sniffer mode on an access point.

Command Default

Local

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The sniffer mode captures and forwards all the packets from the clients on that channel to a remote machine that runs AiroPeek or other supported packet analyzer software. It includes information on the timestamp, signal strength, packet size and so on.

Examples

This example shows how to set the controller to communicate with access point AP01 in local mode:

```
Controller# ap name AP01 mode local submode none
```

This example shows how to set the controller to communicate with access point AP01 in a wired rogue access point detector mode:

```
Controller# ap name AP01 mode rogue
```

This example shows how to set the controller to communicate with access point AP02 in wireless sniffer mode:

```
Controller# ap name AP02 mode sniffer
```

ap name monitor-mode

To configure Cisco lightweight access point channel optimization, use the **ap name monitor-mode** command.

ap name *ap-name* **monitor-mode** {**no-optimization**| **tracking-opt**| **wips-optimized**}

Syntax Description

ap-name	Name of the Cisco lightweight access point.
no-optimization	Specifies no channel scanning optimization for the access point.
tracking-opt	Enables tracking optimized channel scanning for the access point.
wips-optimized	Enables wIPS optimized channel scanning for the access point.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to configure a Cisco wireless intrusion prevention system (wIPS) monitor mode on access point AP01:

```
Controller# ap name AP01 monitor-mode wips
```

ap name monitor-mode dot11b

To configures 802.11b scanning channels for a monitor-mode access point, use the **ap name monitor-mode dot11b** command.

ap name *ap-name* **monitor-mode dot11b fast-channel** *channel1* [*channel2*] [*channel3*] [*channel4*]

Syntax Description

ap-name	Name of the access point.
fast-channel	Specifies the 2.4 GHz band scanning channel (or channels) for a monitor-mode access point.
channel1	Scanning channel1.
channel2	(Optional) Scanning channel2.
channel3	(Optional) Scanning channel3.
channel4	(Optional) Scanning channel4.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to configure an access point in tracking optimized mode to listen to channels 1, 6, and 11:

```
Controller# ap name AP01 monitor-mode dot11b fast-channel 1 6 11
```

ap name name

To modify the name of a Cisco lightweight access point, use the **ap name name** command.

ap name *ap-name* **name** *new-name*

Syntax Description

ap-name	Current Cisco lightweight access point name.
new-name	Desired Cisco lightweight access point name.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to modify the name of access point AP1 to AP2:

```
Controller# ap name AP1 name AP2
```

ap name bridging

To enable Ethernet-to-Ethernet bridging on a Cisco lightweight access point, use the **ap name bridging** command. To disable Ethernet-to-Ethernet bridging on a Cisco lightweight access point, use the **no** form of this command.

ap name *ap-name* **bridging**

ap name *ap-name* **no bridging**

Syntax Description

ap-name	Name of the Cisco lightweight access point.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to enable Ethernet-to-Ethernet bridging on an access point:

```
Controller# ap name TSIM_AP2 bridging
```

ap name cdp interface

To enable the Cisco Discovery Protocol (CDP) on a Cisco lightweight access point, use the **ap name** command. To disable the Cisco Discovery Protocol (CDP) on a Cisco lightweight access point, use the **no** form of this command.

ap name *ap-name* **cdp interface** {**ethernet** *ethernet-id*| **radio** *radio-id*}

ap name *ap-name* [**no**] **cdp interface** {**ethernet** *ethernet-id*| **radio** *radio-id*}

Syntax Description

ap-name	Name of the Cisco lightweight access point.
ethernet	Enables CDP on an Ethernet interface.
ethernet-id	Ethernet interface number from 0 to 3.
radio	Enables CDP for a radio interface.
radio-id	Radio ID slot number from 0 to 3.

Command Default

Disabled on all access points.

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

CDP over Ethernet/radio interfaces is available only when CDP is enabled. After you enable CDP on all access points that are joined to the controller, you can disable and then reenable CDP on individual access points by using the **ap name** *ap-name* **cdp interface ethernet** *ethernet-id* cisco_ap command. After you disable CDP on all access points that are joined to the controller, you cannot enable and then disable CDP on individual access points.

Examples

This example shows how to enable CDP for Ethernet interface number 0 on an access point:

```
Controller# ap name TSIM_AP2 cdp interface ethernet 0
```

ap name console-redirect

To redirect the remote debug output of a Cisco lightweight access point to the console, use the **ap name console-redirect** command. To disable the redirection of the remote debug output of a Cisco lightweight access point to the console, use the **no** form of this command.

ap name *ap-name* **console-redirect**

ap name *ap-name* [**no**] **console-redirect**

Syntax Description

ap-name	Name of the Cisco lightweight access point.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to enable redirecting remote debug output of a Cisco access point named AP02 to the console:

```
Controller# ap name AP02 console-redirect
```

ap name no dot11 shutdown

To enable radio transmission for an individual Cisco radio on an 802.11 network, use the **ap name no dot11 shutdown** command.

ap name *ap-name* **no dot11**{**24ghz**| **5ghz**} **shutdown**

Syntax Description

ap-name	Name of the Cisco lightweight access point.
24ghz	Specifies the 2.4 GHz radios.
5ghz	Specifies the 5 GHz radios.

Command Default

The transmission is enabled for the entire network by default.

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Note Use this command with the **ap name** *Cisco-AP* **dot11 5ghz shutdown** command when configuring 802.11 settings.

This command can be used any time that the CLI interface is active.

Examples

This example shows how to enable radio transmission on the 5 GHz band for access point AP1:

```
Controller# ap name AP1 no dot11 5ghz shutdown
```

ap name link-encryption

To enable Datagram Transport Layer Security (DTLS) data encryption for specific Cisco lightweight access points, use the **ap name link-encryption** command. To disable DTLS data encryption for specific Cisco lightweight access points, use the **no** form of this command.

ap name *ap-name* **link-encryption**

ap name *ap-name* **no link-encryption**

Syntax Description

ap-name	Name of the Cisco lightweight access point.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to enable data encryption for an access point:

```
Controller# ap name AP02 link-encryption
```

ap name link-latency

To enable link latency for a specific Cisco lightweight access point that is currently associated to the controller, use the **ap name link-latency** command. To disable link latency for a specific Cisco lightweight access point that is currently associated to the controller, use the **no** form of this command.

ap name *ap-name* **link-latency**

ap name *ap-name* **no link-latency**

Syntax Description

ap-name	Name of the Cisco lightweight access point.

Command Default

Link latency is disabled by default.

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

This command enables or disables link latency only for access points that are currently joined to the controller. It does not apply to access points that join in the future.

Examples

This example shows how to enable link latency on access points:

```
Controller# ap name AP2 link-latency
```

ap name mfp

To enable management frame protection (MFP), use the **ap name mfp** command. To disable MFP, use the **no** form of this command.

ap name *ap-name* **mfp infrastructure-validation**

ap name *ap-name* **no mfp infrastructure-validation**

Syntax Description

ap-name	Name of the Cisco lightweight access point.
infrastructure-validation	Disables infrastructure validation.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to enable MFP on a Cisco lightweight access point:

```
Controller# ap name AP2 mfp infrastructure-validation
```

ap name power

To enable the Cisco Power over Ethernet (PoE) feature for access points, use the **ap name power** command. To disable the Cisco PoE feature for access points, use the **no** form of this command.

ap name *ap-name* **power** {**injector**| **pre-standard**}

ap name *ap-name* **no power** {**injector**| **pre-standard**}

Syntax Description

ap-name	Name of the Cisco lightweight access point.
injector	Specifies the power injector state for an access point.
pre-standard	Enables the inline power Cisco prestandard switch state for an access point.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to enable the power injector state for all access points:

```
Controller# ap name AP01 power injector
```

This example shows how to enable the inline power Cisco prestandard switch state for access point AP02:

```
Controller# ap name AP02 power pre-standard
```

ap name shutdown

To disable a Cisco lightweight access point, use the **ap name shutdown** command. To enable a Cisco lightweight access point, use the **no** form of this command.

ap name *ap-name* **shutdown**

ap name *ap-name* **no shutdown**

Syntax Description

ap-name	Name of the Cisco lightweight access point.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example how to disable a specific Cisco lightweight access point:

```
Controller# ap name AP2 shutdown
```

ap name slot shutdown

To disable a slot on a Cisco lightweight access point, use the **ap name slot shutdown** command. To enable a slot on a Cisco lightweight access point, use the **no** form of the command.

ap name *ap-name* **slot** {**0**| **1**| **2**| **3**} **shutdown**

ap name *ap-name* **no slot** {**0**| **1**| **2**| **3**} **shutdown**

Syntax Description

ap-name	Name of the Cisco lightweight access point.
0	Enables slot number 0 on a Cisco lightweight access point.
1	Enables slot number 1 on a Cisco lightweight access point.
2	Enables slot number 2 on a Cisco lightweight access point.
3	Enables slot number 3 on a Cisco lightweight access point.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to enable slot 0 on a Cisco access point named TSIM_AP2:

```
Controller# ap name TSIM_AP2 no slot 0 shutdown
```

ap name sniff

To enable sniffing on an access point, use the **ap name sniff** command. To disable sniffing on an access point, use the **no** form of this command.

ap name *ap-name* **sniff** {**dot11a**| **dot11b**}

ap name *ap-name* **no sniff** {**dot11a**| **dot11b**}

Syntax Description

ap-name	Name of the Cisco lightweight access point.
dot11a	Specifies the 2.4 GHz band.
dot11b	Specifies the 5 GHz band.
channel	Valid channel to be sniffed. For the 5 GHz band, the range is 36 to 165. For the 2.4 GHz band, the range is 1 to 14.
server-ip-address	IP address of the remote machine running Omnipeek, Airopeek, AirMagnet, or Wireshark software.

Command Default

Channel 36

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

When the sniffer feature is enabled on an access point, it starts sniffing the signal on the given channel. It captures and forwards all the packets to the remote computer that runs Omnipeek, Airopeek, AirMagnet, or Wireshark software. It includes information about the timestamp, signal strength, packet size and so on.

Before an access point can act as a sniffer, a remote computer that runs one of the listed packet analyzers must be set up so that it can receive packets that are sent by the access point.

Examples

This example shows how to enable the sniffing on the 5 GHz band for an access point on the primary wireless LAN controller:

```
Controller# ap name AP2 sniff dot11a 36 192.0.2.54
```

ap name ssh

To enable Secure Shell (SSH) connectivity on a specific Cisco lightweight access point, use the **ap name ssh** command. To disable SSH connectivity on a specific Cisco lightweight access point, use the **no** form of this command.

ap name *ap-name* **ssh**

ap name *ap-name* **no ssh**

Syntax Description

ap-name	Name of the Cisco lightweight access point.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The Cisco lightweight access point associates with this Cisco controller for all network operations and in the event of a hardware reset.

Examples

This example shows how to enable SSH connectivity on access point Cisco_ap2:

```
Controller# ap name Cisco_ap2 ssh
```

ap name telnet

To enable Telnet connectivity on an access point, use the **ap name telnet** command. To disable Telnet connectivity on an access point, use the **no** form of this command.

ap name *ap-name* **telnet**

ap name *ap-name* **no telnet**

Syntax Description

ap-name	Name of the Cisco lightweight access point.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to disable Telnet connectivity on access point cisco_ap1:

```
Controller# ap name cisco_ap1 no telnet
```

ap name power injector

To configure the power injector state for an access point, use the **ap name power injector** command. To disable the Cisco Power over Ethernet (PoE) feature for access points, use the **no** form of this command.

ap name *ap-name* **power injector** {**installed**| **override**| **switch-mac-address** *switch-MAC-address*}

ap name *ap-name* **no power injector**

Syntax Description

ap-name	Name of he Cisco lightweight access point.
installed	Detects the MAC address of the current switch port that has a power injector.
override	Overrides the safety checks and assumes a power injector is always installed.
switch-mac-address	Specifies the MAC address of the switch port with an installed power injector.
switch-MAC-address	MAC address of the switch port with an installed power injector.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to enable the power injector state for an access point:

```
Controller# ap name AP01 power injector switch-mac-address aaaa.bbbb.cccc
```

ap name power pre-standard

To enable the inline power Cisco prestandard switch state for an access point, use the **ap name power pre-standard** command. To disable the inline power Cisco prestandard switch state for an access point, use the **no** form of this command.

ap name *ap-name* **power pre-standard**

ap name *ap-name* **no power pre-standard**

Syntax Description

ap-name	Name of the Cisco lightweight access point.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to enable the inline power Cisco prestandard switch state for access point AP02:

```
Controller# ap name AP02 power pre-standard
```

This example shows how to disable the inline power Cisco prestandard switch state for access point AP02:

```
Controller# ap name AP02 no power pre-standard
```

ap name reset-button

To configure the Reset button for an access point, use the **ap name reset-button** command.

ap name *ap-name* **reset-button**

Syntax Description

ap-name	Name of the Cisco lightweight access point.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to enable the Reset button for access point AP03:

```
Controller# ap name AP03 reset-button
```

ap name reset

To reset a specific Cisco lightweight access point, use the **ap name reset** command.

ap name *ap-name* **reset**

Syntax Description

ap-name	Name of the Cisco lightweight access point.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to reset a Cisco lightweight access point named AP2:

```
Controller# ap name AP2 reset
```

ap name slot

To configure various slot parameters, use the **ap name slot** command. To disable a slot on a Cisco lightweight access point, use the **no** form of this command.

ap name *ap-name* **slot** *slot-number* {**channel** {**global**| **number** *channel-number*| **width** *channel-width*}| **rtsthreshold** *value*| **shutdown**| **txpower** {**global**| *channel-level*}}

ap name *ap-name* **no slot** {**0**| **1**| **2**| **3**} **shutdown**

Syntax Description

ap-name	Name of the Cisco access point.
slot-number	Slot downlink radio to which the channel is assigned. You can specify the following slot numbers: • **0—**Enables slot number 0 on a Cisco lightweight access point. • **1—**Enables slot number 1 on a Cisco lightweight access point. • **2—**Enables slot number 2 on a Cisco lightweight access point. • **3—**Enables slot number 3 on a Cisco lightweight access point.
channel	Specifies the channel for the slot.
global	Specifies channel global properties for the slot.
number	Specifies the channel number for the slot.
channel-number	Channel number from 1 to 169.
width	Specifies the channel width for the slot.
channel-width	Channel width from 20 to 40.
rtsthreshold	Specifies the RTS/CTS threshold for an access point.
value	RTS/CTS threshold value from 0 to 65535.
shutdown	Shuts down the slot.
txpower	Specifies Tx power for the slot.
global	Specifies auto-RF for the slot.
channel-level	Transmit power level for the slot from 1 to 7.

Command Default

None

Command Modes Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples This example shows how to enable slot 3 for the access point abc:

```
Controller# ap name abc slot 3
```

This example shows how to configure RTS for the access point abc:

```
Controller# ap name abc slot 3 rtsthreshold 54
```

ap name static-ip

To configure lightweight access point static IP settings, use the **ap name static-ip** command. To disable the Cisco lightweight access point static IP address, use the **no** form of this command.

ap name *ap-name* **static-ip** {**domain** *domain-name*| **ip-address** *ip-address* **netmask** *netmask* **gateway** *gateway*| **nameserver** *ip-address*}

ap name *ap-name* **no static-ip**

Syntax Description

ap-name	Name of the access point.
domain	Specifies the Cisco access point domain name.
domain-name	Domain to which a specific access point belongs.
ip-address	Specifies the Cisco access point static IP address.
ip-address	Cisco access point static IP address.
netmask	Specifies the Cisco access point static IP netmask.
netmask	Cisco access point static IP netmask.
gateway	Specifies the Cisco access point gateway.
gateway	IP address of the Cisco access point gateway.
nameserver	Specifies a DNS server so that a specific access point can discover the controller using DNS resolution.
ip-address	IP address of the DNS server.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

An access point cannot discover the controller using Domain Name System (DNS) resolution if a static IP address is configured for the access point unless you specify a DNS server and the domain to which the access point belongs.

Examples

This example shows how to configure an access point static IP address:

```
Controller# ap name AP2 static-ip ip-address 192.0.2.54 netmask 255.255.255.0 gateway
192.0.2.1
```

ap name stats-timer

To set the time in seconds that the Cisco lightweight access point sends its DOT11 statistics to the Cisco controller, use the **ap name stats-timer** command.

ap name *ap-name* **stats-timer** *timer-value*

Syntax Description

ap-name	Name of the Cisco lightweight access point.
timer-value	Time in seconds from 0 to 65535. A zero value disables the timer.

Command Default

0 (Disabled).

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

A value of 0 (zero) means that the Cisco lightweight access point does not send any DOT11 statistics. The acceptable range for the timer is from 0 to 65535 seconds, and the Cisco lightweight access point must be disabled to set this value.

Examples

This example shows how to set the stats timer to 600 seconds for access point AP2:

```
Controller# ap name AP2 stats-timer 600
```

ap name syslog host

To configure a syslog server for a specific Cisco lightweight access point, use the **ap name syslog host** command.

ap name *ap-name* **syslog host** *syslog-host-ip-address*

Syntax Description

ap-name	Name of the Cisco lightweight access point.
syslog-host-ip-address	IP address of the syslog server.

Command Default

255.255.255.255

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

By default, the syslog server IP address for each access point is 255.255.255.255, which indicates that it is not yet set. When the default value is used, the global access point syslog server IP address is pushed to the access point.

Examples

This example shows how to configure a syslog server:

```
Controller# ap name AP2 syslog host 192.0.2.54
```

ap name syslog level

To configure the system logging level, use the **ap name syslog level** command.

ap name *ap-name* **syslog level** {**alert**| **critical**| **debug**| **emergency**| **errors**| **information**| **notification**| **warning**}

Syntax Description

ap-name	Name of the Cisco lightweight access point.
alert	Specifies alert level system logging.
critical	Specifies critical level system logging.
debug	Specifies debug level system logging.
emergency	Specifies emergency level system logging.
errors	Specifies error level system logging.
information	Specifies information level system logging.
notification	Specifies notification level system logging.
warning	Specifies warning level system logging.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to configure alert level system logging:

```
Controller# ap name AP2 syslog level alert
```

ap name tcp-adjust-mss

To enable or disable the TCP maximum segment size (MSS) on a particular access point, use the **ap name tcp-adjust-mss** command. To disable the TCP maximum segment size (MSS) on a particular access point, use the **no** form of this command.

ap name *ap-name* **tcp-adjust-mss size** *size*

ap name *ap-name* **no tcp-adjust-mss**

Syntax Description

ap-name	Name of the access point.
size	Maximum segment size, from 536 to 1363 bytes.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

When you enable this feature, the access point checks for TCP packets to and from wireless clients in its data path. If the MSS of these packets is greater than the value that you configured or greater than the default value for the Control and Provisioning of Wireless Access Points (CAPWAP) tunnel, the access point changes the MSS to the new configured value. If the MSS of these packets is greater than the value that you have configured or greater than the default value for the CAPWAP tunnel, the access point changes the MSS to the newly configured value.

Examples

This example shows how to enable the TCP MSS on access point Cisco_ap1:

```
Controller# ap name ciscoap tcp-adjust-mss size 1200
```

ap name tftp-downgrade

To configure the settings used for downgrading a lightweight access point to an autonomous access point, use the **ap name tftp-downgrade** command.

ap name *ap-name* **tftp-downgrade** *tftp-server-ip filename*

Syntax Description

ap-name	Name of the Cisco lightweight access point.
tftp-server-ip	IP address of the TFTP server.
filename	Filename of the access point image file on the TFTP server.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to configure the settings for downgrading access point AP1:

```
Controller# ap name Ap01 tftp-downgrade 172.21.12.45 ap3g1-k9w7-tar.124-25d.JA.tar
```

ap power injector

To configure the power injector state for all the Cisco lightweight access points that are joined to the controller, use the **ap power injector** command. To delete the power injector state for all access points, use the **no** form of this command.

ap power injector {**installed**| **override**| **switch-mac-address** *switch-MAC-addr*}

no ap power injector

Syntax Description

installed	Detects the MAC address of the current switch port that has a power injector.
override	Overrides the safety checks and assumes a power injector is always installed.
switch-mac-address	Specifies the MAC address of the switch port with an installed power injector.
switch-MAC-address	Specifies the MAC address of the switch port with an installed power injector.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to enable the power injector state for all the Cisco lightweight access points that are joined to the controller:

```
Controller(config)# ap power injector switch-mac-address aaaa.bbbb.cccc
```

ap power pre-standard

To set the Cisco lightweight access points that are joined to the controller to be powered by a high-power Cisco switch, use the **ap power pre-standard** command. To disable the pre standard power for all access points, use the **no** form of this command.

ap power pre-standard

no ap power pre-standard

Syntax Description

This command has no keywords and arguments.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to enable the inline power Cisco prestandard switch state for access point AP02:

```
Controller(config)# ap power pre-standard
```

ap reporting-period

To configure the access point rogue/error reporting period, use the **ap reporting-period** command. To disable the access point rogue/error reporting period, use the **no** form of this command.

ap reporting-period *value*

no ap reporting-period

Syntax Description

value	Time period in seconds from 10 to 120.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example show how to configure the access point rogue/error reporting:

```
Controller(config)# ap reporting-period 100
```

This example show how to disable the access point rogue/error reporting:

```
Controller(config)# no ap reporting-period 100
```

ap reset-button

To configure the Reset button for all Cisco lightweight access points that are joined to the controller, use the **ap reset-button** command. To disable the Reset button for all access points, use the **no** form of this command.

ap reset-button

no ap reset-button

Syntax Description

This command has no keywords and arguments.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to configure the Reset button for all access points that are joined to the controller:

```
Controller(config)# ap reset-button
```

ap static-ip

To configure Cisco lightweight access point static IP address settings, use the **ap static-ip** command. To disable access point static IP settings, use the **no** form of this command.

ap static-ip {**domain** *domain-name*| **name-server** *ip-address*}

no ap static-ip {**domain**| **name-server**}

Syntax Description

domain	Specifies the domain to which a specific access point or all access points belong.
domain-name	Domain name.
name-server	Specifies a DNS server so that a specific access point or all access points can discover the controller using DNS resolution.
ip-address	DNS server IP address.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

An access point cannot discover the controller using Domain Name System (DNS) resolution if a static IP address is configured for the access point, unless you specify a DNS server and the domain to which the access point belongs.

Examples

This example shows how to configure a static IP address for all access points:

```
Controller(config)# ap static-ip domain cisco.com
```

ap syslog

To configure the system logging settings for all Cisco lightweight access points that are joined to the controller, use the **ap syslog** command.

ap syslog {**host** *ipaddress*| **level**{**alert**| **critical**| **debug**| **emergency**| **errors**| **information**| **notification**| **warning**}}

Syntax Description

host	Specifies a global syslog server for all access points that join the controller.
ipaddress	IP address of the syslog server.
level	Specifies the system logging level for all the access points joined to the controller.
alert	Specifies alert level system logging for all Cisco access points.
critical	Specifies critical level system logging for all Cisco access points.
debug	Specifies debug level system logging for all Cisco access points.
emergency	Specifies emergency level system logging for all Cisco access points.
errors	Specifies errors level system logging for all Cisco access points.
information	Specifies information level system logging for all Cisco access points.
notification	Specifies notification level system logging for all Cisco access points.
warning	Specifies warning level system logging for all Cisco access points.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

By default, the global syslog server IP address for all access points is 255.255.255.255. Make sure that the access points can reach the subnet on which the syslog server resides before configuring the syslog server on

the controller. If the access points cannot reach this subnet, the access points are unable to send out syslog messages.

Examples

This example shows how to configure a global syslog server for all access points:

```
Controller(config)# ap syslog host 172.21.34.45
```

ap tcp-adjust-mss size

To enable the TCP maximum segment size (MSS) on all Cisco lightweight access points, use the **ap tcp-adjust-mss size** command. To disable the TCP maximum segment size (MSS) on all Cisco lightweight access points **no** form of this command.

ap tcp-adjust-mss size *size*

no ap tcp-adjust-mss

Syntax Description

size	Maximum segment size, from 536 to 1363 bytes.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

When you enable this feature, the access point checks for TCP packets to and from wireless clients in its data path. If the MSS of these packets is greater than the value that you configured or greater than the default value for the Control and Provisioning of Wireless Access Points (CAPWAP) tunnel, the access point changes the MSS to the new configured value.

Examples

This example shows how to enable the TCP MSS on all access points with a segment size of 1200:

```
Controller(config)# ap tcp-adjust-mss 1200
```

ap tftp-downgrade

To configure the settings used for downgrading a lightweight access point to an autonomous access point, use the **ap tftp-downgrade** command. To disable the settings used for downgrading a lightweight access point to an autonomous access point, use the **no** form of this command.

ap tftp-downgrade *tftp-server-ip filename*

no ap tftp-downgrade

Syntax Description

tftp-server-ip	IP address of the TFTP server.
filename	Filename of the access point image file on the TFTP server.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to configure the settings for downgrading all access points:

```
Controller(config)# ap tftp-downgrade 172.21.23.45 ap3g1-k9w7-tar.124-25d.JA.tar
```

clear ap name tsm dot11 all

To clear the traffic stream metrics (TSM) statistics for a particular access point or all the access points, use the **clear ap name tsm dot11 all** command.

clear ap name *ap-name* **tsm dot11** {**24ghz**| **5ghz**} **all**

Syntax Description

ap-name	Name of the Cisco lightweight access point.
24ghz	Specifies the 2.4 GHz band.
5ghz	Specifies the 5 GHz band.
all	Specifies all access points.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to clear the TSM statistics for an access point on the 2.4 GHz band:

```
Controller# clear ap name AP1 tsm dot11 24ghz all
```

clear ap config

To clear (reset to the default values) a lightweight access point's configuration settings, use the **clear ap config** command.

clear ap config *ap-name* [**eventlog**| **keep-ip-config**]

Syntax Description

ap-name	Name of the Cisco lightweight access point.
eventlog	(Optional) Deletes the existing event log and creates an empty event log file for a specific access point or for all access points joined to the controller.
keep-ip-config	(Optional) Specifies not to erase the static IP configuration of the Cisco access point.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Entering this command does not clear the static IP address of the access point.

Examples

This example shows how to clear the access point's configuration settings for the access point named AP01:

```
Controller# clear ap config AP01
```

clear ap eventlog-all

To delete the existing event log and create an empty event log file for all access points, use the **clear ap eventlog-all** command.

clear ap eventlog-all

Syntax Description

This command has no keywords and arguments.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to delete the event log for all access points:

```
Controller# clear ap eventlog-all
```

clear ap join statistics

To clear the join statistics for all access points or for a specific access point, use the **clear ap join statistics** command.

clear ap join statistics

Syntax Description

This command has no keywords and arguments.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to clear the join statistics of all the access points:

```
Controller# clear ap join statistics
```

clear ap mac-address

To clear the MAC address for the join statistics for a specific Cisco lightweight access point, use the **clear ap mac-address** command.

clear ap mac-address *mac* **join statistics**

Syntax Description

mac	Access point MAC address.
join statistics	Clears join statistics.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to clear the join statistics of an access point:

```
Controller# clear ap mac-address aaaa.bbbb.cccc join statistics
```

clear ap name wlan statistics

To clear WLAN statistics, use the **clear ap name wlan statistics** command.

clear ap name *ap-name* **wlan statistics**

Syntax Description

ap-name	Name of the Cisco lightweight access point.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to clear the WLAN configuration elements of the access point cisco_ap:

```
Controller# clear ap name cisco_ap wlan statistics
```

show ap cac voice

To display the list of all access points with brief voice statistics, which include bandwidth used, maximum bandwidth available, and the call information, use the **show ap cac voice** command.

show ap cac voice

Syntax Description

This command has no keywords and arguments.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to display voice CAC details that correspond to Cisco lightweight access points:

```
controller# show ap cac voice

1) AP Name: AP01
==============================

  Wireless Bandwidth (In MeanTime mt)

       Slot#  Radio         Calls  BW-Max  BW-Alloc  Bw-InUse (%age)
  ------------------------------------------------------------------
  1    0      802.11b/g     0      23437   0         0
  2    1      802.11a       0      23437   0         0

  Wired Bandwidth (in Kbps)

       Slot#  Wlan-ID  Wlan-Name             BW-Config   BW-Avail
  ------------------------------------------------------------------
  1    0      1        maria-open            0           0
  2    0      12       24                    0           0
  3    1      1        maria-open            0           0
  4    1      12       24                    0           0


2) AP Name: AP02
==============================

  Wireless Bandwidth (In MeanTime mt)

       Slot#  Radio         Calls  BW-Max  BW-Alloc  Bw-InUse (%age)
  ------------------------------------------------------------------
  1    0      802.11b/g     0      23437   0         0
  2    1      802.11a       0      23437   0         0

  Wired Bandwidth (in Kbps)
```

```
     Slot#  Wlan-ID  Wlan-Name             BW-Config   BW-Avail
-------------------------------------------------------------------
1    0      1        maria-open            0           0
2    0      12       24                    0           0
3    1      1        maria-open            0           0
4    1      12       24                    0           0
```

show ap capwap

To display the Control and Provisioning of Wireless Access Points (CAPWAP) configuration that is applied to all access points, use the **show ap capwap** command.

show ap capwap {**retransmit**| **timers**| **summary**}

Syntax Description

retransmit	Displays the access point CAPWAP retransmit parameters.
timers	Displays the rogue access point entry timers.
summary	Displays the network configuration of the Cisco controller.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to display the access point CAPWAP retransmit parameters:

```
Controller# show ap capwap retransmit

Global control packet retransmit interval : 3
Global control packet retransmit count : 5

AP Name                          Retransmit Interval           Retransmit Count
-----------------------------------------------------------------------------
AP01                              3                             5

AP02                              3                             5

AP03                              3                             5

AP04                              3                             5

AP05                              3                             5

AP07                              3                             5

AP08                              3                             5

AP09                              3                             5

AP10                              3                             5

AP11                              3                             5
```

```
AP12                                3                                   5
```

This example shows how to display the rogue access point entry timers:

```
Controller# show ap capwap timers

AP Discovery timer       : 10
AP Heart Beat timeout    : 30
Primary Discovery timer  : 120
Primed Join timeout      : 0
Fast Heartbeat           : Disabled
Fast Heartbeat timeout   : 1
```

This example shows how to display the the network configuration of the Cisco controller:

```
Controller# show ap capwap summary

AP Fallback                      : Enabled
AP Join Priority                 : Disabled
AP Master                        : Disabled
Primary backup Controller Name   :
Primary backup Controller IP     : 0.0.0.0
Secondary backup Controller Name :
Secondary backup Controller IP   : 0.0.0.0
```

show ap cdp

To display the Cisco Discovery Protocol (CDP) information for all Cisco lightweight access points that are joined to the controller, use the **show ap cdp** command.

show ap cdp [**neighbors** [**detail**]]

Syntax Description

neighbors	(Optional) Displays neighbors using CDP.
detail	(Optional) Displays details about a specific access point neighbor that is using CDP.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to display the CDP status of all access points:

```
Controller# show ap cdp
```

This example shows how to display details about all neighbors that are using CDP:

```
Controller# show ap cdp neighbors
```

show ap config dot11

To display the detailed configuration of 802.11-58G radios on Cisco lightweight access points, use the **show ap config dot11** command.

show ap config dot11 58ghz summary

Syntax Description

58ghz	Displays the 802.11-58G radios.
summary	Displays a summary of the radios on the access points.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to display the detailed configuration of 802.11a-58G radios on access points:

```
Controller# show ap config dot11 58ghz summary
```

show ap config

To display configuration settings for all access points that join the controller, use the **show ap config** command.

show ap config {**ethernet**| **general**| **global**}

Syntax Description

ethernet	Displays ethernet VLAN tagging information for all Cisco APs.
general	Displays common information for all Cisco APs.
global	Displays global settings for all Cisco APs.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to display global syslog server settings:

```
Controller# show ap config global
AP global system logging host                   : 255.255.255.255
```

show ap crash-file

To display the list of both crash and radio core dump files generated by lightweight access points, use the **show ap crash-file** command.

show ap crash-file

Syntax Description

This command has no keywords and arguments.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to display the crash file generated by the access point:

```
Controller# show ap crash-file
```

show ap data-plane

To display the data plane status, use the **show ap data-plane** command.

show ap data-plane

Syntax Description

This command has no keywords and arguments.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example show how to display the data plane status for all access points:

```
Controller# show ap data-plane
```

show ap dot11 l2roam

To display 802.11a or 802.11b/g Layer 2 client roaming information, use the **show ap dot11 l2roam** command.

show ap dot11 {**24ghz**| **5ghz**} **l2roam** {**mac-address** *mac-address* **statistics**| **rf-param**| **statistics**}

Syntax Description

24ghz	Specifies the 2.4 GHz band.
5ghz	Specifies the 5 GHz band.
mac-address *mac-address* **statistics**	Specifies the MAC address of a Cisco lightweight access point.
rf-param	Specifies the Layer 2 frequency parameters.
statistics	Specifies the Layer 2 client roaming statistics.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to display 802.11b Layer 2 client roaming information:

```
Controller# show ap dot11 24ghz l2roam rf-param

L2Roam 802.11bg RF Parameters
  Config Mode          : Default
  Minimum RSSI         : -85
  Roam Hysteresis      : 2
  Scan Threshold       : -72
  Transition time      : 5
```

show ap dot11 cleanair air-quality

To display the air-quality summary information and air-quality worst information for the 802.11 networks, use the **show ap dot11 cleanair air-quality** command.

show ap dot11 {**24ghz**| **5ghz**} **cleanair air-quality** {**summary**| **worst**}

Syntax Description

24ghz	Displays the 2.4 GHz band.
5ghz	Displays the 5 GHz band.
summary	Displays a summary of 802.11 radio band air-quality information.
worst	Displays the worst air-quality information for 802.11 networks.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to display the worst air-quality information for the 5 GHz band:

```
Controller# show ap dot11 5ghz cleanair air-quality worst

AQ = Air Quality
DFS = Dynamic Frequency Selection
AP Name      Channel Avg AQ Min AQ Interferers DFS
------------ ------- ------ ------ ----------- -----
CISCO_AP3500 36      95     70     0           40
```

This example shows how to display the worst air-quality information for the 2.4 GHz band:

```
Controller# show ap dot11 24ghz cleanair air-quality worst

AQ = Air Quality
DFS = Dynamic Frequency Selection
AP Name      Channel Avg AQ Min AQ Interferers DFS
------------ ------- ------ ------ ----------- -----
CISCO_AP3500 1       83     57     3           5
```

show ap dot11 cleanair config

To display the CleanAir configuration for the 802.11 networks, use the **show ap dot11 cleanair config** command.

show ap dot11 {**24ghz**| **5ghz**} **cleanair config**

Syntax Description

24ghz	Displays the 2.4 GHz band.
5ghz	Displays the 5 GHz band.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to display the CleanAir configuration for the 2.4 GHz band:

```
Controller# show ap dot11 24ghz cleanair config
Clean Air Solution................................ : Disabled
Air Quality Settings:
    Air Quality Reporting......................... : Disabled
    Air Quality Reporting Period (min)............ : 15
    Air Quality Alarms............................ : Enabled
    Air Quality Alarm Threshold................... : 10
Interference Device Settings:
    Interference Device Reporting................. : Enabled
        Bluetooth Link............................ : Enabled
        Microwave Oven............................ : Enabled
        802.11 FH................................. : Enabled
        Bluetooth Discovery....................... : Enabled
        TDD Transmitter........................... : Enabled
        Jammer.................................... : Enabled
        Continuous Transmitter.................... : Enabled
        DECT-like Phone........................... : Enabled
        Video Camera.............................. : Enabled
        802.15.4.................................. : Enabled
        WiFi Inverted............................. : Enabled
        WiFi Invalid Channel...................... : Enabled
        SuperAG................................... : Enabled
        Canopy.................................... : Enabled
        Microsoft Device.......................... : Enabled
        WiMax Mobile.............................. : Enabled
        WiMax Fixed............................... : Enabled
    Interference Device Types Triggering Alarms:
        Bluetooth Link............................ : Disabled
        Microwave Oven............................ : Disabled
        802.11 FH................................. : Disabled
```

```
        Bluetooth Discovery..................... : Disabled
        TDD Transmitter......................... : Disabled
        Jammer.................................. : Disabled
        Continuous Transmitter.................. : Disabled
        DECT-like Phone......................... : Disabled
        Video Camera............................ : Disabled
        802.15.4................................ : Disabled
        WiFi Inverted........................... : Enabled
        WiFi Invalid Channel.................... : Enabled
        SuperAG................................. : Disabled
        Canopy.................................. : Disabled
        Microsoft Device........................ : Disabled
        WiMax Mobile............................ : Disabled
        WiMax Fixed............................. : Disabled
    Interference Device Alarms.................. : Enabled
Additional Clean Air Settings:
    CleanAir Event-driven RRM State............. : Disabled
    CleanAir Driven RRM Sensitivity............. : LOW
    CleanAir Persistent Devices state........... : Disabled
```

show ap dot11

To display 802.11a or 802.11b configuration information, use the **show ap dot11** command.

show ap dot11 {**24ghz**| **5ghz**} {**channel**| **coverage**| **group**| **logging**| **media-stream**| **monitor**| **network**| **profile**| **receiver**| **service-policy**| **summary**| **txpower**| **ccx global**}

Syntax Description

24ghz	Specifies the 2.4 GHz band.
5ghz	Specifies the 5 GHz band.
channel	Displays the automatic channel assignment configuration and statistics.
coverage	Displays the configuration and statistics for coverage hole detection.
group	Displays 802.11a or 802.11b Cisco radio RF grouping.
logging	Displays 802.11a or 802.11b RF event and performance logging.
media-stream	Display 802.11a or 802.11b Media Resource Reservation Control configurations.
monitor	Displays the 802.11a or 802.11b default Cisco radio monitoring.
network	Displays the 802.11a or 802.11b network configuration.
profile	Displays the 802.11a or 802.11b lightweight access point performance profiles.
receiver	Displays the configuration and statistics of the 802.11a or 802.11b receiver.
service-policy	Displays the Quality of Service (QoS) service policies for 802.11a or 802.11b radio for all Cisco access points.
summary	Displays the 802.11a or 802.11b Cisco lightweight access point name, channel, and transmit level summary.
txpower	Displays the 802.11a or 802.11b automatic transmit power assignment.
ccx global	Displays 802.11a or 802.11b Cisco Client eXtensions (CCX) information for all Cisco access points that are joined to the controller.

Command Default None

Command Modes Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples This example shows how to display the automatic channel assignment configuration and statistics:

```
Controller# show ap dot11 5ghz channel
Automatic Channel Assignment
  Channel Assignment Mode                  : AUTO
  Channel Update Interval                  : 12 Hours
  Anchor time (Hour of the day)            : 20
  Channel Update Contribution              : SNI.
  Channel Assignment Leader                : web (9.9.9.2)
  Last Run                                 : 13105 seconds ago
  DCA Sensitivity Level                    : MEDIUM (15 dB)
  DCA 802.11n Channel Width                : 40 Mhz
  Channel Energy Levels
      Minimum                              : unknown
      Average                              : unknown
      Maximum                              : unknown
  Channel Dwell Times
      Minimum                              : unknown
      Average                              : unknown
      Maximum                              : unknown
  802.11a 5 GHz Auto-RF Channel List
  Allowed Channel List                     : 36,40,44,48,52,56,60,64,149,153,1
57,161
  Unused Channel List                      : 100,104,108,112,116,132,136,140,1
65
  802.11a 4.9 GHz Auto-RF Channel List
  Allowed Channel List                     :
  Unused Channel List                      : 1,2,3,4,5,6,7,8,9,10,11,12,13,14,
15,16,17,18,19,20,21,22,23,24,25,26
  DCA Outdoor AP option                    : Disabled
```

This example shows how to display the statistics for coverage hole detection:

```
Controller# show ap dot11 5ghz coverage
Coverage Hole Detection
  802.11a Coverage Hole Detection Mode          : Enabled
  802.11a Coverage Voice Packet Count           : 100 packet(s)
  802.11a Coverage Voice Packet Percentage      : 50 %
  802.11a Coverage Voice RSSI Threshold         : -80dBm
  802.11a Coverage Data Packet Count            : 50 packet(s)
  802.11a Coverage Data Packet Percentage       : 50 %
  802.11a Coverage Data RSSI Threshold          : -80dBm
  802.11a Global coverage exception level       : 25
  802.11a Global client minimum exception level   : 3 clients
```

This example shows how to display Cisco radio RF group settings:

```
Controller# show ap dot11 5ghz group
Radio RF Grouping

  802.11a Group Mode                : STATIC
  802.11a Group Update Interval     : 600 seconds
```

```
  802.11a Group Leader               : web (10.10.10.1)
  802.11a Group Member               : web(10.10.10.1)
                                       nb1(172.13.21.45) (*Unreachable)
  802.11a Last Run                   : 438 seconds ago


  Mobility Agents RF membership information
  ------------------------------------------------------------
  No of 802.11a MA RF-members : 0
```

This example shows how to display 802.11a RF event and performance logging:

```
Controller# show ap dot11 5ghz logging
RF Event and Performance Logging

  Channel Update Logging             : Off
  Coverage Profile Logging           : Off
  Foreign Profile Logging            : Off
  Load Profile Logging               : Off
  Noise Profile Logging              : Off
  Performance Profile Logging        : Off
  TxPower Update Logging             : Off
```

This example shows how to display the 802.11a media stream configuration:

```
Controller# show ap dot11 5ghz media-stream
Multicast-direct                : Disabled
Best Effort                     : Disabled
Video Re-Direct                 : Disabled
Max Allowed Streams Per Radio     : Auto
Max Allowed Streams Per Client    : Auto
Max Video Bandwidth              : 0
Max Voice Bandwidth              : 75
Max Media Bandwidth              : 85
Min PHY Rate (Kbps)              : 6000
Max Retry Percentage             : 80
```

This example shows how to display the radio monitoring for the 802.11b network:

```
Controller# show ap dot11 5ghz monitor
Default 802.11a AP monitoring

  802.11a Monitor Mode                         : Enabled
  802.11a Monitor Mode for Mesh AP Backhaul    : disabled
  802.11a Monitor Channels                     : Country channels
  802.11a RRM Neighbor Discover Type           : Transparent
  802.11a AP Coverage Interval                 : 180 seconds
  802.11a AP Load Interval                     : 60 seconds
  802.11a AP Noise Interval                    : 180 seconds
  802.11a AP Signal Strength Interval          : 60 seconds
```

This example shows how to display the global configuration and statistics of an 802.11a profile:

```
Controller# show ap dot11 5ghz profile
Default 802.11a AP performance profiles
802.11a Global Interference threshold.............. 10%
802.11a Global noise threshold..................... -70 dBm
802.11a Global RF utilization threshold............ 80%
802.11a Global throughput threshold................ 1000000 bps
802.11a Global clients threshold................... 12 clients
802.11a Global coverage threshold.................. 12 dB
802.11a Global coverage exception level............ 80%
802.11a Global client minimum exception lev........ 3 clients
```

This example shows how to display the network configuration of an 802.11a profile:

```
Controller# show ap dot11 5ghz network
802.11a Network : Enabled
11nSupport : Enabled
  802.11a Low Band : Enabled
  802.11a Mid Band : Enabled
  802.11a High Band : Enabled
```

```
802.11a Operational Rates
  802.11a 6M : Mandatory
  802.11a 9M : Supported
  802.11a 12M : Mandatory
  802.11a 18M : Supported
  802.11a 24M : Mandatory
  802.11a 36M : Supported
  802.11a 48M : Supported
  802.11a 54M : Supported
802.11n MCS Settings:
  MCS 0 : Supported
  MCS 1 : Supported
  MCS 2 : Supported
  MCS 3 : Supported
  MCS 4 : Supported
  MCS 5 : Supported
  MCS 6 : Supported
  MCS 7 : Supported
  MCS 8 : Supported
  MCS 9 : Supported
  MCS 10 : Supported
  MCS 11 : Supported
  MCS 12 : Supported
  MCS 13 : Supported
  MCS 14 : Supported
  MCS 15 : Supported
  MCS 16 : Supported
  MCS 17 : Supported
  MCS 18 : Supported
  MCS 19 : Supported
  MCS 20 : Supported
  MCS 21 : Supported
  MCS 22 : Supported
  MCS 23 : Supported
802.11n Status:
  A-MPDU Tx:
    Priority 0 : Enabled
    Priority 1 : Disabled
    Priority 2 : Disabled
    Priority 3 : Disabled
    Priority 4 : Enabled
    Priority 5 : Enabled
    Priority 6 : Disabled
    Priority 7 : Disabled
  A-MSDU Tx:
    Priority 0 : Enabled
    Priority 1 : Enabled
    Priority 2 : Enabled
    Priority 3 : Enabled
    Priority 4 : Enabled
    Priority 5 : Enabled
    Priority 6 : Disabled
    Priority 7 : Disabled
  Guard Interval : Any
  Rifs Rx : Enabled
Beacon Interval : 100
CF Pollable mandatory : Disabled
CF Poll Request Mandatory : Disabled
CFP Period : 4
CFP Maximum Duration : 60
Default Channel : 36
Default Tx Power Level : 1
DTPC Status : Enabled
Fragmentation Threshold : 2346
Pico-Cell Status : Disabled
Pico-Cell-V2 Status : Disabled
TI Threshold : 0
Legacy Tx Beamforming setting : Disabled
Traffic Stream Metrics Status : Disabled
Expedited BW Request Status : Disabled
EDCA profile type check : default-wmm
Call Admision Control (CAC) configuration
Voice AC
```

```
  Voice AC - Admission control (ACM) : Disabled
  Voice Stream-Size : 84000
  Voice Max-Streams : 2
  Voice Max RF Bandwidth : 75
  Voice Reserved Roaming Bandwidth : 6
  Voice Load-Based CAC mode : Enabled
  Voice tspec inactivity timeout : Enabled
CAC SIP-Voice configuration
  SIP based CAC : Disabled
  SIP call bandwidth : 64
  SIP call bandwith sample-size : 20
Video AC
  Video AC - Admission control (ACM) : Disabled
  Video max RF bandwidth : Infinite
  Video reserved roaming bandwidth : 0
```

This example shows how to display the global configuration and statistics of an 802.11a profile:

```
Controller# show ap dot11 5ghz receiver
Default 802.11a AP performance profiles
802.11a Global Interference threshold.............. 10%
802.11a Global noise threshold..................... -70 dBm
802.11a Global RF utilization threshold............ 80%
802.11a Global throughput threshold................ 1000000 bps
802.11a Global clients threshold................... 12 clients
802.11a Global coverage threshold.................. 12 dB
802.11a Global coverage exception level............ 80%
802.11a Global client minimum exception lev........ 3 clients
```

This example shows how to display the global configuration and statistics of an 802.11a profile:

```
Controller# show ap dot11 5ghz service-policy
```

This example shows how to display a summary of the 802.11b access point settings:

```
Controller# show ap dot11 5ghz summary
AP Name MAC Address       Admin State Operation State Channel TxPower
------- ----------------- ----------- --------------- ------- -------
CJ-1240 00:21:1b:ea:36:60 ENABLED     UP              161     1( )
CJ-1130 00:1f:ca:cf:b6:60 ENABLED     UP              56*     1(*)
```

This example shows how to display the configuration and statistics of the 802.11a transmit power cost:

```
Controller# show ap dot11 5ghz txpower
Automatic Transmit Power Assignment

Transmit Power Assignment Mode          : AUTO
Transmit Power Update Interval          : 600 seconds
Transmit Power Threshold                : -70 dBm
Transmit Power Neighbor Count           : 3 APs
Min Transmit Power                      : -10 dBm
Max Transmit Power                      : 30 dBm
Transmit Power Update Contribution      : SNI.
Transmit Power Assignment Leader        : web (10.10.10.1)
Last Run                                : 437 seconds ago
```

This example shows how to display the configuration and statistics of the 802.11a transmit power cost:

```
Controller# show ap dot11 5ghz ccx global
 802.11a Client Beacon Measurements:
     disabled
```

show ap ethernet statistics

To display Ethernet statistics for all Cisco lightweight access points, use the **show ap ethernet statistics** command.

show ap ethernet statistics

Syntax Description

This command has no keywords and arguments.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to display Ethernet statistics for all access points:

```
Controller# show ap ethernet statistics
```

show ap groups

To display information about all access point groups that are defined in the system, use the **show ap groups** command.

show ap groups

Syntax Description

This command has no keywords and arguments.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to display information about all access point groups:

```
Controller# show ap groups
```

show ap image

To display the images present on Cisco lightweight access points, use the **show ap image** command.

show ap image

Syntax Description

This command has no keywords and arguments.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to display images on the access points:

```
Controller# show ap image
```

show ap join stats summary

To display the last join error detail for a specific access point, use the **show ap join stats summary** command.

show ap join stats summary

Syntax Description

This command has no keywords and arguments.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

To obtain the MAC address of the 802.11 radio interface, enter the **show interface** command on the access point.

Examples

This example shows how to display specific join information for an access point:

```
Controller# show ap join stats summary
Number of APs : 1

Base MAC        Ethernet MAC    AP Name                IP Address       Status

--------------- --------------- ---------------------- ---------------- -------------
-
c8f9.f91a.aa80  0000.0000.0000  N A                    0.0.0.0          Not Joined
```

show ap link-encryption

To display the link encryption status, use the **show ap link-encryption** command.

show ap link-encryption

Syntax Description

This command has no keywords and arguments.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example show how to display the link-encryption status:

```
Controller# show ap link-encryption
```

show ap mac-address

To display join-related statistics collected and last join error details for access points, use the **show ap mac-address** command.

show ap mac-address *mac-address* **join stats** {**detailed**| **summary**}

Syntax Description

mac-address	Access point Ethernet MAC address or the MAC address of the 802.11 radio interface.
join stats	Displays join information and statistics for Cisco access points.
detailed	Displays all join-related statistics collected.
summary	Displays the last join error detail.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to display join information for a specific access point that is trying to join the controller:

```
Controller# show ap mac-address d0c2.8267.8b00 join stats detailed

Discovery phase statistics
  Discovery requests received                            : 6
  Successful discovery responses sent                    : 6
  Unsuccessful discovery request processing              : 0
  Reason for last unsuccessful discovery attempt         : Not applicable
  Time at last successful discovery attempt              : Nov 20 17:25:10.841
  Time at last unsuccessful discovery attempt            : Not applicable

Join phase statistics
  Join requests received                                 : 3
  Successful join responses sent                         : 3
  Unsuccessful join request processing                   : 0
  Reason for last unsuccessful join attempt              : Not applicable
  Time at last successful join attempt                   : Nov 20 17:25:20.998
  Time at last unsuccessful join attempt                 : Not applicable

Configuration phase statistics
  Configuration requests received                        : 8
  Successful configuration responses sent                : 3
  Unsuccessful configuration request processing          : 0
```

```
  Reason for last unsuccessful configuration attempt      : Not applicable
  Time at last successful configuration attempt           : Nov 20 17:25:21.177
  Time at last unsuccessful configuration attempt         : Not applicable

Last AP message decryption failure details
  Reason for last message decryption failure              : Not applicable

Last AP disconnect details
  Reason for last AP connection failure                  : Number of message retransmission
 to the AP has reached maximum

Last join error summary
  Type of error that occurred last                        : AP got or has been disconnected

  Reason for error that occurred last                    : Number of message retransmission
 to the AP has reached maximum
  Time at which the last join error occurred              : Nov 20 17:22:36.438
```

This example shows how to display specific join information for an access point:

```
Controller# show ap mac-address d0c2.8267.8b00 join stats detailed

Is the AP currently connected to controller..... No
Time at which the AP joined this controller last time..... Aug 21 12:50:36:061
Type of error that occurred last..... Lwapp join request
rejected
Reason for error that occurred last..... RADIUS authorization
is pending for the AP
Time at which the last join error occurred..... Aug 21 12:50:34:374
```

show ap monitor-mode summary

To display the current channel-optimized monitor mode settings, use the **show ap monitor-mode summary** command.

show ap monitor-mode summary

Syntax Description

This command has no keywords and arguments.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to display current channel-optimized monitor mode settings:

```
Controller# show ap monitor-mode summary

AP Name Ethernet MAC      Status   Scanning Channel List
------- -------------     -------- -------- ----------------
AP_004  xx:xx:xx:xx:xx:xx Tracking 1,6,11,  4
```

show ap name auto-rf

To display the auto-RF settings for a Cisco lightweight access point, use the **show ap name auto-rf** command.

show ap name *ap-name* **auto-rf dot11** {**24ghz**| **5ghz**}

Syntax Description

ap-name	Name of the Cisco lightweight access point.
24ghz	Displays the 2.4 GHz band.
5ghz	Displays the 5 GHz band.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to display auto-RF information for an access point:

```
Controller# show ap name AP01 auto-rf dot11 24ghz

Number of Slots                                 : 2
AP Name                                         : TSIM_AP-1
MAC Address                                     : 0000.2000.02f0
Slot ID                                         : 0
Radio Type                                      : 802.11b/g
Subband Type                                    : All

Noise Information
  Noise Profile                                 : Failed
  Channel   1                                    :   24 dBm
  Channel   2                                    :   48 dBm
  Channel   3                                    :   72 dBm
  Channel   4                                    :   96 dBm
  Channel   5                                    :  120 dBm
  Channel   6                                    : -112 dBm
  Channel   7                                    :  -88 dBm
  Channel   8                                    :  -64 dBm
  Channel   9                                    :  -40 dBm
  Channel  10                                    :  -16 dBm
  Channel  11                                    :    8 dBm

Interference Information
  Interference Profile                          : Passed
  Channel   1                                    : -128 dBm @  0% busy
  Channel   2                                    :  -71 dBm @  1% busy
  Channel   3                                    :  -72 dBm @  1% busy
  Channel   4                                    :  -73 dBm @  2% busy
```

```
  Channel   5                                     :  -74 dBm @  3% busy
  Channel   6                                     :  -75 dBm @  4% busy
  Channel   7                                     :  -76 dBm @  5% busy
  Channel   8                                     :  -77 dBm @  5% busy
  Channel   9                                     :  -78 dBm @  6% busy
  Channel  10                                     :  -79 dBm @  7% busy
  Channel  11                                     :  -80 dBm @  8% busy

Load Information
  Load Profile                                    : Passed
  Receive Utilization                             : 10%
  Transmit Utilization                            : 20%
  Channel Utilization                             : 50%
  Attached Clients                                : 0 clients

Coverage Information
  Coverage Profile                                : Passed
  Failed Clients                                  : 0 clients

Client Signal Strengths
  RSSI -100 dBm                                   : 0 clients
  RSSI  -92 dBm                                   : 0 clients
  RSSI  -84 dBm                                   : 0 clients
  RSSI  -76 dBm                                   : 0 clients
  RSSI  -68 dBm                                   : 0 clients
  RSSI  -60 dBm                                   : 0 clients
  RSSI  -52 dBm                                   : 0 clients

Client Signal to Noise Ratios
  SNR    0 dB                                     : 0 clients
  SNR    5 dB                                     : 0 clients
  SNR   10 dB                                     : 0 clients
  SNR   15 dB                                     : 0 clients
  SNR   20 dB                                     : 0 clients
  SNR   25 dB                                     : 0 clients
  SNR   30 dB                                     : 0 clients
  SNR   35 dB                                     : 0 clients
  SNR   40 dB                                     : 0 clients
  SNR   45 dB                                     : 0 clients

Nearby APs
  AP 0000.2000.0300 slot 0                        : -68 dBm on  11 (10.10.10.1)
  AP 0000.2000.0400 slot 0                        : -68 dBm on  11 (10.10.10.1)
  AP 0000.2000.0600 slot 0                        : -68 dBm on  11 (10.10.10.1)

Radar Information

Channel Assignment Information
  Current Channel Average Energy                  : 0 dBm
  Previous Channel Average Energy                 : 0 dBm
  Channel Change Count                            : 0
  Last Channel Change Time                        : Wed Oct 17 08:13:36 2012
  Recommended Best Channel                        : 11

RF Parameter Recommendations
  Power Level                                     : 1
  RTS/CTS Threshold                               : 2347
  Fragmentation Threshold                         : 2346
  Antenna Pattern                                 : 0

Persistent Interference Devices
```

show ap name bhmode

To display Cisco bridge backhaul mode, use the **show ap name bhmode** command.

show ap name *ap-name* **bhmode**

Syntax Description

ap-name	Name of the Cisco lightweight access point.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to display Cisco bridge backhaul mode of an access point:

```
Controller# show ap name TSIM_AP-1 bhmode
```

show ap name bhrate

To display the Cisco bridge backhaul rate, use the **show ap name bhrate** command.

show ap name *ap-name* **bhrate**

Syntax Description

ap-name	Name of the Cisco lightweight access point.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to display the Cisco bridge backhaul rate for an access point:

```
Controller# show ap name AP01 bhrate
```

show ap name cac voice

To display voice call admission control details for a specific Cisco lightweight access point, use the **show ap name cac voice** command.

show ap name *ap-name* **cac voice**

Syntax Description

ap-name	Name of the Cisco lightweight access point.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to display voice call admission control details for an access point:

```
Controller# show ap name AP01 cac voice
1) AP Name: AP01
============================

  Wireless Bandwidth (In MeanTime mt)

       Slot#  Radio         Calls  BW-Max  BW-Alloc  Bw-InUse (%age)
  ------------------------------------------------------------------
  1    0      802.11b/g     0      23437   0         0
  2    1      802.11a       0      23437   0         0

  Wired Bandwidth (in Kbps)

       Slot#  Wlan-ID  Wlan-Name             BW-Config   BW-Avail
  ------------------------------------------------------------------
  1    0      1        maria-open            0           0
  2    0      12       24                    0           0
  3    1      1        maria-open            0           0
  4    1      12       24                    0           0
```

show ap name dot11 call-control

To display call control information and the metrics for successful calls, use the **show ap name dot11 call-control** command.

show ap name *ap-name* **dot11** {**24ghz**| **5ghz**} **call-control** {**call-info**| **metrics**}

Syntax Description

ap-name	Name of the Cisco lightweight access point
24ghz	Displays the 2.4 GHz band.
5ghz	Displays the 5 GHz band.
call-info	Displays call information.
metrics	Displays call metrics.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to display metrics for successful calls for an access point:

```
Controller# show ap name AP01 dot11 24ghz call-control metrics

Slot#   Call Count      Call Duration
---------------------------------
0       0               0
```

show ap name capwap retransmit

To display Control and Provisioning of Wireless Access Points (CAPWAP) retransmit settings, use the **show ap name capwap retransmit** command.

show ap name *ap-name* **capwap retransmit**

Syntax Description

ap-name	Name of the Cisco lightweight access point.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to display CAPWAP retransmit settings of an access point:

```
Controller# show ap name AP01 capwap retransmit

AP Name   Retransmit Interval Retransmit Count
--------  ------------------- ----------------
AP01      3                   5
```

show ap name ccx rm

To display an access point's Cisco Client eXtensions (CCX) radio management status information, use the **show ap name ccx rm** command.

show ap name *ap-name* **ccx rm status**

Syntax Description

ap-name	Name of the Cisco lightweight access point.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to display CCX radio management information for an access point:

```
Controller# show ap name AP01 ccx rm status

802.11b/g Radio
  Beacon Request                                : Disabled
  Channel Load Request                          : Disabled
  Frame Request                                 : Disabled
  Noise Histogram Request                       : Disabled
  Path Loss Request                             : Disabled
  Interval                                      : 60
  Iteration                                     : 0

802.11a Radio
  Beacon Request                                : Disabled
  Channel Load Request                          : Disabled
  Frame Request                                 : Disabled
  Noise Histogram Request                       : Disabled
  Path Loss Request                             : Disabled
  Interval                                      : 60
  Iteration                                     : 0
```

show ap name cdp

To display the Cisco Discovery Protocol (CDP) information for an access point, use the **show ap name cdp** command.

show ap name *ap-name* **cdp** [**neighbors** [**detail**]]

Syntax Description

ap-name	Name of the Cisco lightweight access point.
neighbors	(Optional) Displays neighbors that are using CDP.
detail	(Optional) Displays details about a specific access point neighbor that is using CDP.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to display CDP information for an access point:

```
Controller# show ap name AP01 cdp neighbors detail
```

show ap name channel

To display the available channels for a specific mesh access point, use the **show ap name channel** command.

show ap name *ap-name* **channel**

Syntax Description

ap-name	Name of the Cisco lightweight access point.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to display the available channels for a particular access point:

```
Controller# show ap name AP01 channel

Slot ID                                          : 0
Allowed Channel List                             : 1, 2, 3, 4, 5, 6, 7, 8, 9
                                                   10, 11
Slot ID                                          : 1
Allowed Channel List                             : 36, 40, 44, 48, 52, 56, 60, 64, 100
                                                   104, 108, 112, 116, 132, 136, 140, 149,
 153
                                                   157, 161
```

show ap name config

To display common information and Ethernet VLAN tagging information for a specific Cisco lightweight access point, use the **show ap name config** command.

show ap name *ap-name* **config** {**ethernet**| **general**}

Syntax Description

ap-name	Name of the Cisco lightweight access point.
ethernet	Displays Ethernet tagging configuration information for an access point.
general	Displays common information for an access point.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to display Ethernet tagging information for an access point:

```
Controller# show ap name AP01 config ethernet

VLAN Tagging Information for AP01
```

This example shows how to display common information for an access point:

```
Controller# show ap name AP01 config general

Cisco AP Name                                  : AP01
Cisco AP Identifier                            : 5
Country Code                                   : US  - United States
Regulatory Domain Allowed by Country           : 802.11bg:-A     802.11a:-A
AP Country Code                                : US  - United States
AP Regulatory Domain                           : Unconfigured
Switch Port Number                             : Te1/0/1
MAC Address                                    : 0000.2000.02f0
IP Address Configuration                       : Static IP assigned
IP Address                                     : 10.10.10.12
IP Netmask                                     : 255.255.0.0
Gateway IP Address                             : 10.10.10.1
Fallback IP Address Being Used                 : 10.10.10.12
Domain                                         : Cisco
Name Server                                    : 0.0.0.0
CAPWAP Path MTU                                : 1485
Telnet State                                   : Enabled
SSH State                                      : Disabled
Cisco AP Location                              : sanjose
```

```
Cisco AP Group Name                             : default-group
Primary Cisco Controller Name                   : CAPWAP Controller
Primary Cisco Controller IP Address             : 10.10.10.1
Secondary Cisco Controller Name                 :
Secondary Cisco Controller IP Address           : Not Configured
Tertiary Cisco Controller Name                  :
Tertiary Cisco Controller IP Address            : Not Configured
Administrative State                            : Enabled
Operation State                                 : Registered
AP Mode                                         : Local
AP Submode                                      : Not Configured
Remote AP Debug                                 : Disabled
Logging Trap Severity Level                     : informational
Software Version                                : 7.4.0.5
Boot Version                                    : 7.4.0.5
Stats Reporting Period                          : 180
LED State                                       : Enabled
PoE Pre-Standard Switch                         : Disabled
PoE Power Injector MAC Address                  : Disabled
Power Type/Mode                                 : Power Injector/Normal Mode
Number of Slots                                 : 2
AP Model                                        : 1140AG
AP Image                                        : C1140-K9W8-M
IOS Version                                     :
Reset Button                                    :
AP Serial Number                                : SIM1140K001
AP Certificate Type                             : Manufacture Installed
Management Frame Protection Validation          : Disabled
AP User Mode                                    : Customized
AP User Name                                    : cisco
AP 802.1X User Mode                             : Not Configured
AP 802.1X User Name                             : Not Configured
Cisco AP System Logging Host                    : 255.255.255.255
AP Up Time                                      : 15 days 16 hours 19 minutes 57
 seconds
AP CAPWAP Up Time                               : 4 minutes 56 seconds
Join Date and Time                              : 10/18/2012 04:48:56
Join Taken Time                                 : 15 days 16 hours 15 minutes 0
seconds
Join Priority                                   : 1
Ethernet Port Duplex                            : Auto
Ethernet Port Speed                             : Auto
AP Link Latency                                 : Disabled
Rogue Detection                                 : Disabled
AP TCP MSS Adjust                               : Disabled
AP TCP MSS Size                                 : 6146
```

show ap name config dot11

To display 802.11 configuration information that corresponds to specific Cisco lightweight access points, use the **show ap name config dot11** command.

show ap name *ap-name* **config dot11** {**24ghz**| **49ghz**| **58ghz**| **5hgz**}

Syntax Description

ap-name	Name of the Cisco lightweight access point.
24ghz	Displays the 2.4 GHz band.
49ghz	Displays 802.11-4.9G network settings.
58ghz	Displays 802.11-5.8G network settings.
5hgz	Displays the 5 GHz band.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to display 802.11b configuration information that corresponds to a specific Cisco lightweight access point:

```
Controller# show ap name AP01 config dot11 24ghz

Cisco AP Identifier                             : 5
Cisco AP Name                                   : AP01
Country Code                                    : US  - United States
Regulatory Domain Allowed by Country            : 802.11bg:-A     802.11a:-A
AP Country Code                                 : US  - United States
AP Regulatory Domain                            : -A
Switch Port Number                              : Te1/0/1
MAC Address                                     : 0000.2000.02f0
IP Address Configuration                        : Static IP assigned
IP Address                                      : 10.10.10.12
IP Netmask                                      : 255.255.0.0
Gateway IP Address                              : 10.10.10.1
Fallback IP Address Being Used                  : 10.10.10.12
Domain                                          : Cisco
Name Server                                     : 0.0.0.0
CAPWAP Path MTU                                 : 1485
Telnet State                                    : Enabled
SSH State                                       : Disabled
```

```
Cisco AP Location                               : sanjose
Cisco AP Group Name                             : default-group
Administrative State                            : Enabled
Operation State                                 : Registered
AP Mode                                         : Local
AP Submode                                      : Not Configured
Remote AP Debug                                 : Disabled
Logging Trap Severity Level                     : informational
Software Version                                : 7.4.0.5
Boot Version                                    : 7.4.0.5
Mini IOS Version                                : 3.0.51.0
Stats Reporting Period                          : 180
LED State                                       : Enabled
PoE Pre-Standard Switch                         : Disabled
PoE Power Injector MAC Address                  : Disabled
Power Type/Mode                                 : Power Injector/Normal Mode
Number of Slots                                 : 2
AP Model                                        : 1140AG
AP Image                                        : C1140-K9W8-M
IOS Version                                     :
Reset Button                                    :
AP Serial Number                                : SIM1140K001
AP Certificate Type                             : Manufacture Installed
Management Frame Protection Validation          : Disabled
AP User Mode                                    : Customized
AP User Name                                    : cisco
AP 802.1X User Mode                             : Not Configured
AP 802.1X User Name                             : Not Configured
Cisco AP System Logging Host                    : 255.255.255.255
AP Up Time                                      : 15 days 17 hours 9 minutes 41
seconds
AP CAPWAP Up Time                               : 54 minutes 40 seconds
Join Date and Time                              : 10/18/2012 04:48:56
Join Taken Time                                 : 15 days 16 hours 15 minutes 0
seconds

Attributes for Slot 0
  Radio Type                                    : 802.11n - 2.4 GHz
  Administrative State                          : Enabled
  Operation State                               : Up
  Cell ID                                       : 0

  Station Configuration
    Configuration                               : Automatic
    Number of WLANs                             : 1
    Medium Occupancy Limit                      : 100
    CFP Period                                  : 4
    CFP Maximum Duration                        : 60
    BSSID                                       : 000020000200

    Operation Rate Set
       1000 Kbps                                : MANDATORY
       2000 Kbps                                : MANDATORY
       5500 Kbps                                : MANDATORY
      11000 Kbps                                : MANDATORY
       6000 Kbps                                : SUPPORTED
       9000 Kbps                                : SUPPORTED
      12000 Kbps                                : SUPPORTED
      18000 Kbps                                : SUPPORTED
      24000 Kbps                                : SUPPORTED
      36000 Kbps                                : SUPPORTED
      48000 Kbps                                : SUPPORTED
      54000 Kbps                                : SUPPORTED

    MCS Set
      MCS  0                                    : SUPPORTED
      MCS  1                                    : SUPPORTED
      MCS  2                                    : SUPPORTED
      MCS  3                                    : SUPPORTED
      MCS  4                                    : SUPPORTED
      MCS  5                                    : SUPPORTED
      MCS  6                                    : SUPPORTED
      MCS  7                                    : SUPPORTED
```

```
    MCS  8                                    : SUPPORTED
    MCS  9                                    : SUPPORTED
    MCS 10                                    : SUPPORTED
    MCS 11                                    : SUPPORTED
    MCS 12                                    : SUPPORTED
    MCS 13                                    : SUPPORTED
    MCS 14                                    : SUPPORTED
    MCS 15                                    : SUPPORTED
    MCS 16                                    : DISABLED
    MCS 17                                    : DISABLED
    MCS 18                                    : DISABLED
    MCS 19                                    : DISABLED
    MCS 20                                    : DISABLED
    MCS 21                                    : DISABLED
    MCS 22                                    : DISABLED
    MCS 23                                    : DISABLED

  Beacon Period                               : 100
  Fragmentation Threshold                     : 2346
  Multi Domain Capability Implemented         : True
  Multi Domain Capability Enabled             : True
  Country String                              : US

Multi Domain Capability
  Configuration                               : Automatic
  First Channel                               : 0
  Number of Channels                          : 0
  Country String                              : US

MAC Operation Parameters
  Configuration                               : Automatic
  Fragmentation Threshold                     : 2346
  Packet Retry Limit                          : 64
  Legacy Tx Beamforming Setting               : Disabled

Tx Power
  Number of Supported Power Levels            : 8
  Tx Power Level 1                            : 20 dBm
  Tx Power Level 2                            : 17 dBm
  Tx Power Level 3                            : 14 dBm
  Tx Power Level 4                            : 11 dBm
  Tx Power Level 5                            : 8 dBm
  Tx Power Level 6                            : 5 dBm
  Tx Power Level 7                            : 2 dBm
  Tx Power Level 8                            : -1 dBm
  Tx Power Configuration                      : Automatic
  Current Tx Power Level                      : 1

Phy OFDM Parameters
  Configuration                               : Automatic
  Current Channel                             : 11
  Extension Channel                           : None
  Channel Width                               : 20 MHz
  Allowed Channel List                        : 1, 2, 3, 4, 5, 6, 7, 8, 9
                                                10, 11
  TI Threshold                                : 0
  Antenna Type                                : Internal
  Internal Antenna Gain (in .5 dBi units)     : 0
  Diversity                                   : Diversity enabled

  802.11n Antennas
    Tx                                        : A, B, C
    Rx                                        : A, B, C

Performance Profile Parameters
  Configuration                               : Automatic
  Interference Threshold                      : 10%
  Noise Threshold                             : -70 dBm
  RF Utilization Threshold                    : 80%
  Data Rate Threshold                         : 1000000 bps
  Client Threshold                            : 12 clients
  Coverage SNR Threshold                      : 15 dB
  Coverage Exception Level                    : 25%
```

```
    Client Minimum Exception Level              : 3 clients
    RTS/CTS Threshold                             : 2347
    Short Retry Limit                             : 7
    Long Retry Limit                              : 4
    Max Tx MSDU Lifetime                          : 512
    Max Rx Lifetime                               : 512

  CleanAir Management Information
    CleanAir Capable                            : Yes
    CleanAir Management Admin State             : Enabled
    CleanAir Management Operation State         : Up
    Rapid Udpate Mode                           : Disabled
    Spectrum Expert connection                  : Disabled
    CleanAir NSI Key                            : 377313C8F290E246E640C4EF177BED
88
    Spectrum Expert connections counter         : 0
    CleanAir Sensor State                       : Configured

  Rogue Containment Information
    Containment Count                           : 0
```

show ap name config slot

To display configuration information for slots on a specific Cisco lightweight access point, use the **show ap name config slot** command.

show ap name *ap-name* **config slot** {**0**| **1**| **2**| **3**}

Syntax Description

ap-name	Name of the Cisco lightweight access point.
0	Displays slot number 0.
1	Displays slot number 1.
2	Displays slot number 2.
3	Displays slot number 3.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to display configuration information for slots on an access point:

```
Controller# show ap name AP01 config slot 0

Cisco AP Identifier                             : 3
Cisco AP Name                                   : AP01
Country Code                                    : US  - United States
Regulatory Domain Allowed by Country            : 802.11bg:-A     802.11a:-A
AP Country Code                                 : US  - United States
AP Regulatory Domain                            : -A
Switch Port Number                              : Te1/0/1
MAC Address                                     : 0000.2000.02f0
IP Address Configuration                        : Static IP assigned
IP Address                                      : 10.10.10.12
IP Netmask                                      : 255.255.0.0
Gateway IP Address                              : 10.10.10.1
Fallback IP Address Being Used                  : 10.10.10.12
Domain                                          : Cisco
Name Server                                     : 0.0.0.0
CAPWAP Path MTU                                 : 1485
Telnet State                                    : Enabled
SSH State                                       : Disabled
Cisco AP Location                               : sanjose
Cisco AP Group Name                             : default-group
```

```
Administrative State                            : Enabled
Operation State                                 : Registered
AP Mode                                         : Local
AP Submode                                      : Not Configured
Remote AP Debug                                 : Disabled
Logging Trap Severity Level                     : informational
Software Version                                : 7.4.0.5
Boot Version                                    : 7.4.0.5
Mini IOS Version                                : 3.0.51.0
Stats Reporting Period                          : 180
LED State                                       : Enabled
PoE Pre-Standard Switch                         : Disabled
PoE Power Injector MAC Address                  : Disabled
Power Type/Mode                                 : Power Injector/Normal Mode
Number of Slots                                 : 2
AP Model                                        : 1140AG
AP Image                                        : C1140-K9W8-M
IOS Version                                     :
Reset Button                                    :
AP Serial Number                                : SIM1140K001
AP Certificate Type                             : Manufacture Installed
Management Frame Protection Validation          : Disabled
AP User Mode                                    : Customized
AP User Name                                    : cisco
AP 802.1X User Mode                             : Not Configured
AP 802.1X User Name                             : Not Configured
Cisco AP System Logging Host                    : 255.255.255.255
AP Up Time                                      : 15 days 16 hours 1 minute 19 s
econds
AP CAPWAP Up Time                               : 20 hours 21 minutes 37 seconds

Join Date and Time                              : 10/17/2012 08:13:36
Join Taken Time                                 : 14 days 19 hours 39 minutes 41
 seconds

Attributes for Slot 0
  Radio Type                                    : 802.11n - 2.4 GHz
  Administrative State                          : Enabled
  Operation State                               : Up
  Cell ID                                       : 0

  Station Configuration
    Configuration                               : Automatic
    Number of WLANs                             : 1
    Medium Occupancy Limit                      : 100
    CFP Period                                  : 4
    CFP Maximum Duration                        : 60
    BSSID                                       : 000020000200

    Operation Rate Set
       1000 Kbps                                : MANDATORY
       2000 Kbps                                : MANDATORY
       5500 Kbps                                : MANDATORY
      11000 Kbps                                : MANDATORY
       6000 Kbps                                : SUPPORTED
       9000 Kbps                                : SUPPORTED
      12000 Kbps                                : SUPPORTED
      18000 Kbps                                : SUPPORTED
      24000 Kbps                                : SUPPORTED
      36000 Kbps                                : SUPPORTED
      48000 Kbps                                : SUPPORTED
      54000 Kbps                                : SUPPORTED

    MCS Set
      MCS  0                                    : SUPPORTED
      MCS  1                                    : SUPPORTED
      MCS  2                                    : SUPPORTED
      MCS  3                                    : SUPPORTED
      MCS  4                                    : SUPPORTED
      MCS  5                                    : SUPPORTED
      MCS  6                                    : SUPPORTED
      MCS  7                                    : SUPPORTED
      MCS  8                                    : SUPPORTED
```

```
    MCS  9                                    : SUPPORTED
    MCS 10                                    : SUPPORTED
    MCS 11                                    : SUPPORTED
    MCS 12                                    : SUPPORTED
    MCS 13                                    : SUPPORTED
    MCS 14                                    : SUPPORTED
    MCS 15                                    : SUPPORTED
    MCS 16                                    : DISABLED
    MCS 17                                    : DISABLED
    MCS 18                                    : DISABLED
    MCS 19                                    : DISABLED
    MCS 20                                    : DISABLED
    MCS 21                                    : DISABLED
    MCS 22                                    : DISABLED
    MCS 23                                    : DISABLED

  Beacon Period                               : 100
  Fragmentation Threshold                     : 2346
  Multi Domain Capability Implemented         : True
  Multi Domain Capability Enabled             : True
  Country String                              : US

Multi Domain Capability
  Configuration                               : Automatic
  First Channel                               : 0
  Number of Channels                          : 0
  Country String                              : US

MAC Operation Parameters
  Configuration                               : Automatic
  Fragmentation Threshold                     : 2346
  Packet Retry Limit                          : 64

Tx Power
  Number of Supported Power Levels            : 8
  Tx Power Level 1                            : 20 dBm
  Tx Power Level 2                            : 17 dBm
  Tx Power Level 3                            : 14 dBm
  Tx Power Level 4                            : 11 dBm
  Tx Power Level 5                            : 8 dBm
  Tx Power Level 6                            : 5 dBm
  Tx Power Level 7                            : 2 dBm
  Tx Power Level 8                            : -1 dBm
  Tx Power Configuration                      : Automatic
  Current Tx Power Level                      : 1

Phy OFDM Parameters
  Configuration                               : Automatic
  Current Channel                             : 11
  Extension Channel                           : None
  Channel Width                               : 20 MHz
  Allowed Channel List                        : 1, 2, 3, 4, 5, 6, 7, 8, 9
                                                10, 11
  TI Threshold                                : 0
  Antenna Type                                : Internal
  Internal Antenna Gain (in .5 dBi units)     : 0
  Diversity                                   : Diversity enabled

  802.11n Antennas
    Tx                                        : A, B, C
    Rx                                        : A, B, C

Performance Profile Parameters
  Configuration                               : Automatic
  Interference Threshold                      : 10%
  Noise Threshold                             : -70 dBm
  RF Utilization Threshold                    : 80%
  Data Rate Threshold                         : 1000000 bps
  Client Threshold                            : 12 clients
  Coverage SNR Threshold                      : 15 dB
  Coverage Exception Level                    : 25%
  Client Minimum Exception Level              : 3 clients
```

```
Rogue Containment Information
  Containment Count                          : 0
```

show ap name core-dump

To display the memory core dump information for a lightweight access point, use the **show ap name core-dump** command.

show ap name *ap-name* **core-dump**

Syntax Description

ap-name	Name of the Cisco lightweight access point.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to display the memory core dump information:

```
Controller# show ap name 3602a core-dump

TFTP server IP : 172.31.25.21
Memory core dump file : 3602a.dump
Memory core dump file compressed : Disabled
```

show ap name data-plane

To display the data plane status of a specific Cisco lightweight access point, use the **show ap name data-plane** command.

show ap name *ap-name* **data-plane**

Syntax Description

ap-name	Name of the Cisco lightweight access point.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to display the data plane status of an access point:

```
Controller# show ap name AP01 data-plane

                      Min Data          Data          Max Data     Last
AP Name              Round Trip     Round Trip     Round Trip    Update
------------------  -------------  -------------  ------------- --------
AP01                   0.000s         0.000s         0.000s       00:00:00
```

show ap name dot11

To display 802.11a or 802.11b configuration information that corresponds to specific Cisco lightweight access points, use the **show ap name dot11** command.

show ap name *ap-name* **dot11** {**24ghz**| **5ghz**} {**ccx**| **cdp**| **profile**| **service-poicy output**| **stats**| **tsm** {**all**| *client-mac*}}

Syntax Description

ap-name	Name of the Cisco lightweight access point.
24ghz	Displays the 2.4 GHz band.
5ghz	Displays the 5 GHz band.
ccx	Displays the Cisco Client eXtensions (CCX) radio management status information.
cdp	Displays Cisco Discovery Protocol (CDP) information.
profile	Displays configuration and statistics of 802.11 profiling.
service-policy output	Displays downstream service policy information.
stats	Displays Cisco lightweight access point statistics.
tsm	Displays 802.11 traffic stream metrics statistics.
all	Displays the list of all access points to which the client has associations.
client-mac	MAC address of the client.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to display the service policy that is associated with the access point:

```
Controller# show ap name test-ap dot11 24ghz service-policy output

Policy Name  : test-ap1
```

```
Policy State : Installed
```

This example shows how to display the CCX RRM 802.11 configuration for a specific access point:

```
Controller# show ap name AP01 dot11 24ghz ccx
```

This example show how to display CDP information for a specific access point:

```
Controller# show ap name AP01 dot11 24ghz cdp

AP Name               AP CDP State
--------------------- --------------
AP03                  Disabled
```

This example show how to display the configuration and statistics of 802.11b profiling for a specific access point:

```
Controller# show ap name AP01 dot11 24ghz profile

 802.11b Cisco AP performance profile mode            : GLOBAL
 802.11b Cisco AP Interference threshold              : 10 %
 802.11b Cisco AP noise threshold                     : -70 dBm
 802.11b Cisco AP RF utilization threshold            : 80 %
 802.11b Cisco AP throughput threshold                : 1000000 bps
 802.11b Cisco AP clients threshold                   : 12 clients
```

This example show how to display downstream service policy information for a specific access point:

```
Controller# show ap name AP01 dot11 24ghz service-policy output

Policy Name  : def-11gn
Policy State : Installed
```

This example show how to display statistics for a specific access point:

```
Controller# show ap name AP01 dot11 24ghz stats

Number of Users................................: 0
TxFragmentCount................................: 0
MulticastTxFrameCnt............................: 0
FailedCount....................................: 0
RetryCount.....................................: 0
MultipleRetryCount.............................: 0
FrameDuplicateCount............................: 0
RtsSuccessCount................................: 0
RtsFailureCount................................: 0
AckFailureCount................................: 0
RxIncompleteFragment...........................: 0
MulticastRxFrameCnt............................: 0
FcsErrorCount..................................: 0
TxFrameCount...................................: 0
WepUndecryptableCount..........................: 0
TxFramesDropped................................: 0

Call Admission Control (CAC) Stats
  Voice Bandwidth in use(% of config bw).........: 0
  Video Bandwidth in use(% of config bw).........: 0
  Total BW in use for Voice(%)...................: 0
  Total BW in use for SIP Preferred call(%)......: 0

Load based Voice Call Stats
  Total channel MT free..........................: 0
  Total voice MT free............................: 0
  Na Direct......................................: 0
  Na Roam........................................: 0

WMM TSPEC CAC Call Stats
  Total num of voice calls in progress...........: 0
  Num of roaming voice calls in progress.........: 0
  Total Num of voice calls since AP joined.......: 0
  Total Num of roaming calls since AP joined.....: 0
```

```
  Total Num of exp bw requests received.....: 0
  Total Num of exp bw requests admitted.....: 0
  Num of voice calls rejected since AP joined....: 0
  Num of roam calls rejected since AP joined.....: 0
  Num of calls rejected due to insufficent bw....: 0
  Num of calls rejected due to invalid params....: 0
  Num of calls rejected due to PHY rate.....: 0
  Num of calls rejected due to QoS policy.....: 0

SIP CAC Call Stats
  Total Num of calls in progress.....: 0
  Num of roaming calls in progress.....: 0
  Total Num of calls since AP joined.....: 0
  Total Num of roaming calls since AP joined.....: 0
  Total Num of Preferred calls received.....: 0
  Total Num of Preferred calls accepted.....: 0
  Total Num of ongoing Preferred calls.....: 0
  Total Num of calls rejected(Insuff BW).....: 0
  Total Num of roam calls rejected(Insuff BW)....: 0

Band Select Stats
  Num of dual band client .....: 0
  Num of dual band client added.....: 0
  Num of dual band client expired .....: 0
  Num of dual band client replaced.....: 0
  Num of dual band client detected .....: 0
  Num of suppressed client .....: 0
  Num of suppressed client expired.....: 0
  Num of suppressed client replaced.....: 0
```

This example show how to display the traffic stream configuration for all clients that correspond to a specific access point:

```
Controller# show ap name AP01 dot11 24ghz tsm all
```

show ap name dot11 cleanair

To display CleanAir configuration information that corresponds to an access point, use the **show ap name dot11 cleanair** command.

show ap name *ap-name* **dot11** {**24ghz**| **5ghz**} **cleanair** {**air-quality**| **device**}

Syntax Description

ap-name	Name of the Cisco lightweight access point.
24ghz	Displays the 2.4 GHz band.
5ghz	Displays the 5 GHz band.
cleanair	Displays CleanAir configuration information.
air-quality	Displays CleanAir air-quality (AQ) data.
device	Displays CleanAir interferers for an access point on the 5 GHz band.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to display CleanAir air-quality information for an access point in the 802.11b network:

```
Controller# show ap name AP01 dot11 24ghz cleanair air-quality

AQ = Air Quality
DFS = Dynamic Frequency Selection
```

This example shows how to display CleanAir interferers information for an access point in the 802.11b network:

```
Controller# show ap name AP01 dot11 24ghz cleanair device

DC    = Duty Cycle (%)
ISI   = Interference Severity Index (1-Low Interference, 100-High Interference)
RSSI  = Received Signal Strength Index (dBm)
DevID = Device ID

No ClusterID DevID Type AP Name ISI RSSI DC Channel
-- --------- ----- ---- ------- --- ---- ----------
```

show ap name ethernet statistics

To display the Ethernet statistics of a specific Cisco lightweight access point, use the **show ap name ethernet statistics** command.

show ap name *ap-name* **ethernet statistics**

Syntax Description

ap-name	Name of the Cisco lightweight access point.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to display the Ethernet statistics of an access point:

```
Controller# show ap name 3602a ethernet statistics

Ethernet Stats for AP 3602a

Interface Name      Status   Speed       Rx Packets    Tx Packets    Discarded Packets

-------------------------------------------------------------------------------------
GigabitEthernet0    UP       1000 Mbps   3793          5036          0
```

show ap name eventlog

To download and display the event log of a specific Cisco lightweight access point, use the **show ap name eventlog** command.

show ap name *ap-name* **eventlog**

Syntax Description

ap-name	Name of the Cisco lightweight access point.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to display the event log for a specific access point:

```
Controller# show ap name AP01 eventlog
```

show ap name image

To display the detailed information about the predownloaded image for specified access points, use the **show ap name image** command.

show ap name *ap-name* **image**

Syntax Description

ap-name	Name of the Cisco lightweight access point.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to display images present on all access points:

```
Controller# show ap name 3602a image

Total number of APs  : 1

Number of APs
        Initiated                   : 0
        Predownloading              : 0
        Completed predownloading    : 0
        Not Supported               : 1
        Failed to Predownload       : 0

AP Name      Primary Image   Backup Image    Predownload Status    Predownload Ver...  Next
 Retry Time    Retry Count
-------------------------------------------------------------------------------------------------
3602a        10.0.1.234      0.0.0.0         Not supported         None                NA
                         0
```

show ap name inventory

To display inventory information for an access point, use the **show ap name inventory** command.

show ap name *ap-name* **inventory**

Syntax Description

ap-name	Name of the Cisco lightweight access point.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to display inventory information for an access point:

```
Controller# show ap name 3502b inventory

NAME: Cisco AP    , DESCR: Cisco Wireless Access Point
PID: 1140AG  ,  VID: V01,  SN: SIM1140K001


NAME:     , DESCR:
PID: ,  VID: ,  SN:


NAME:     , DESCR:
PID: ,  VID: ,  SN:
NAME: Cisco AP    , DESCR: Cisco Wireless Access Point
PID: 3502I  ,  VID: V01,  SN: FTX1525E94A


NAME: Dot11Radio0    , DESCR: 802.11N 2.4GHz Radio
PID: UNKNOWN,  VID:  ,  SN: FOC1522BLNA


NAME: Dot11Radio1    , DESCR: 802.11N 5GHz Radio
PID: UNKNOWN,  VID:  ,  SN: FOC1522BLNA
```

show ap name link-encryption

To display the link-encryption status for a specific Cisco lightweight access point, use the **show ap name link-encryption** command.

show ap name *ap-name* **link-encryption**

Syntax Description

ap-name	Name of the Cisco lightweight access point.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to display the link-encryption status for a specific Cisco lightweight access point:

```
Controller# show ap name AP01 link-encryption

                    Encryption  Dnstream  Upstream    Last
AP Name                  State     Count     Count  Update
------------------  ----------  --------  --------  ------
AP01                 Disabled         0         0   Never
```

show ap name service-policy

To display service-policy information for a specific Cisco lightweight access point, use the **show ap name service-policy** command.

show ap name *ap-name* **service-policy**

Syntax Description

ap-name	Name of the Cisco lightweight access point.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to display service-policy information for a specific Cisco lightweight access point:

```
Controller# show ap name 3502b service-policy

NAME: Cisco AP    , DESCR: Cisco Wireless Access Point
PID: 3502I  ,  VID: V01,  SN: FTX1525E94A


NAME: Dot11Radio0    , DESCR: 802.11N 2.4GHz Radio
PID: UNKNOWN,  VID:  ,  SN: FOC1522BLNA


NAME: Dot11Radio1    , DESCR: 802.11N 5GHz Radio
PID: UNKNOWN,  VID:  ,  SN: FOC1522BLNA
```

show ap name tcp-adjust-mss

To display TCP maximum segment size (MSS) for an access point, use the **show ap name tcp-adjust-mss** command.

show ap name *ap-name* **tcp-adjust-mss**

Syntax Description

ap-name	Name of the Cisco lightweight access point.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to display TCP MSS for an access point:

```
Controller# show ap name AP01 tcp-adjust-mss

AP Name                     TCP State        MSS Size
-----------------------------------------------------
AP01                        Disabled         6146
```

show ap name wlan

To display the Basic Service Set Identifier (BSSID) value for each WLAN defined on an access point and to display WLAN statistics, use the **show ap name wlan** command.

show ap name *ap-name* **wlan** {**dot11** {**24ghz**| **5ghz**}| **statistic**}

Syntax Description

ap-name	Name of the Cisco lightweight access point.
dot11	Displays 802.11 parameters.
24ghz	Displays 802.11b network settings.
5ghz	Displays 802.11a network settings.
statistic	Displays WLAN statistics.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to display BSSID information of an access point in an 802.11b network:

```
Controller# show ap name AP01 wlan dot11 24ghz

Site Name                                       : default-group
Site Description                                :

WLAN ID  Interface  BSSID
------------------------------------
1        default    00:00:20:00:02:00
12       default    00:00:20:00:02:0b
```

This example shows how to display WLAN statistics for an access point:

```
Controller# show ap name AP01 wlan statistic

WLAN ID  : 1
WLAN Profile Name  : maria-open

   EAP Id Request Msg Timeouts           : 0
   EAP Id Request Msg Timeouts Failures  : 0
   EAP Request Msg Timeouts              : 0
   EAP Request Msg Timeouts Failures     : 0
   EAP Key Msg Timeouts                  : 0
```

```
   EAP Key Msg Timeouts Failures         : 0


WLAN ID  : 12
WLAN Profile Name  : 24

   EAP Id Request Msg Timeouts           : 0
   EAP Id Request Msg Timeouts Failures  : 0
   EAP Request Msg Timeouts              : 0
   EAP Request Msg Timeouts Failures     : 0
   EAP Key Msg Timeouts                  : 0
   EAP Key Msg Timeouts Failures         : 0
```

show ap slots

To display a slot summary of all connected Cisco lightweight access points, use the **show ap slots** command.

show ap slots

Syntax Description

This command has no keywords and arguments.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to display a slot summary of all connected Cisco lightweight access points:

```
Controller# show ap slots

AP Name    Slots  AP Model    Slot0       Slot1      Slot2     Slot3
---------- ------ ----------- ----------- ---------- --------- --------
3602a      2      3502I       802.11b/g   802.11a    Unknown   Unknown
```

show ap summary

To display the status summary of all Cisco lightweight access points attached to the controller, use the **show ap summary** command.

show ap summary

Syntax Description

This command has no keywords and arguments.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Use this command to display a list that contains each lightweight access point name, number of slots, manufacturer, MAC address, location, and the controller port number.

Examples

This example shows how to display a summary of all connected access points:

```
Controller# show ap summary

Number of APs: 1

Global AP User Name: Cisco
Global AP Dot1x User Name: Not configured

AP Name                          AP Model  Ethernet MAC    Radio MAC       State
-----------------------------------------------------------------------------------
3602a                            3502I     003a.99eb.3fa8  d0c2.8267.8b00  Registered
```

show ap tcp-adjust-mss

To display information about the Cisco lightweight access point TCP Maximum Segment Size (MSS), use the **show ap tcp-adjust-mss** command.

show ap tcp-adjust-mss

Syntax Description

This command has no keywords and arguments.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to display information about the access point TCP MSS information:

```
Controller# show ap tcp-adjust-mss

AP Name                    TCP State        MSS Size
-----------------------------------------------------
3602a                      Disabled         0
```

show ap uptime

To display the up time of all connected Cisco lightweight access points, use the **show ap uptime** command.

show ap uptime

Syntax Description

This command has no keywords and arguments.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to the display up time of all connected access points:

```
Controller# show ap uptime

Number of APs : 1

Global AP User Name : Cisco
Global AP Dot1x User Name : Not configured

AP Name Ethernet MAC    AP Up Time                      Association Up Time

------- --------------- ------------------------------- ------------------------------
3602a   003a.99eb.3fa8  5 hours 13 minutes 40 seconds  5 hours 12 minutes 15 seconds
```

show wireless client ap

To display the clients on a Cisco lightweight access point, use the **show wireless client ap** command.

show wireless client ap [**name** *ap-name*] **dot11** {**24ghz**| **5ghz**}

Syntax Description

name *ap-name*	(Optional) Displays the name of the Cisco lightweight access point.
dot11	Displays 802.11 parameters.
24ghz	Displays the 2.4 GHz band.
5ghz	Displays the 5 GHz band.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The **show client ap** command might list the status of automatically disabled clients. Use the **show exclusionlist** command to view clients on the exclusion list (blacklisted).

Examples

This example shows how to display client information on a specific Cisco lightweight access point in the 2.4 GHz band:

```
Controller# show wireless client ap name AP01 dot11 24ghz

MAC Address       AP Id  Status     WLAN Id Authenticated
----------------- ------ ---------- ------- -------------
xx:xx:xx:xx:xx:xx 1      Associated 1       No
```

test ap name

To enable automatic testing of the path Maximum Transmit Unit (MTU) between the access point and the controller, use the **test ap name** command.

test ap name *ap-name* **pmtu** {**disable size** *size*| **enable**}

Syntax Description

ap-name	Name of the target Cisco lightweight access point.
pmtu	Tests the MTU configuration for the access point.
disable	Disables path MTU testing and manually configures the MTU value in bytes.
size *size*	Specifies the path MTU size. **Note** The range is from 576 to 1700.
enable	Enables the path MTU testing for the access point.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to disable the path MTU configuration for all access points associated to the controller:

```
Controller# test ap name 3602a pmtu enable
```

test capwap ap name

To test Control and Provisioning of Wireless Access Points (CAPWAP) parameters for a specific Cisco lightweight access points, use the **test capwap ap name** command.

test capwap ap name *ap-name* {**encryption** {**enable| disable**}| **message** *token*}

Syntax Description

ap-name	Name of the Cisco lightweight access point.
encryption	Tests the Datagram Transport Layer Security (DTLS) encryption.
enable	Tests if DTLS encryption is enabled.
disable	Tests if DTLS encryption is disabled.
message *token*	Specifies an RRM neighbor message to send.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to test if DTLS encryption is enabled for a specific access point:

```
Controller# test capwap ap name 3602a encryption enable
```

This example shows how to test if DTLS encryption is disabled for a specific access point:

```
Controller# test capwap ap name 3602a encryption disable
```

trapflags ap

To enable the sending of specific Cisco lightweight access point traps, use the **trapflags ap** command. To disable the sending of Cisco lightweight access point traps, use the **no** form of this command.

trapflags ap {**register**| **interfaceup**}

no trapflags ap {**register**| **interfaceup**}

Syntax Description

register	Enables sending a trap when a Cisco lightweight access point registers with a Cisco switch.
interfaceup	Enables sending a trap when a Cisco lightweight access point interface (A or B) comes up.

Command Default

Enabled

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to prevent traps from sending access point-related traps:

```
Controller(config)# no trapflags ap register
```

PART XII

CleanAir

CleanAir Commands

ap dot11 24ghz cleanair

To enable CleanAir for detecting 2.4 GHz devices, use the **ap dot11 24ghz cleanair** command.

ap dot11 24ghz cleanair

Command Default

Disabled

Command Modes

Global configuration.

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Enable CleanAir first to be able to use the other commands within it.

Examples

This example shows how to enable CleanAir for 2.4 GHz devices

```
Controller(config)#ap dot11 24ghz cleanair
```

ap dot11 24ghz cleanair alarm air-quality

To configure the alarm for the threshold value of air-quality for all 2.4-GHz devices, use the **ap dot11 24ghz cleanair alarm air-quality** command.

ap dot11 24ghz cleanair alarm air-quality threshold *threshold _value*

Syntax Description

air-quality	Configures the alarm for the air-quality of 2.4 GHz devices.
threshold *threshold _value*	Configures the threshold value for air-quality.

Command Default

Disabled

Command Modes

Global configuration.

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Enable CleanAir first to be able to use the other commands within it.

Examples

This example shows how to set the threshold value for the air-quality.

```
Controller(config)#ap dot11 24ghz cleanair alarm air-quality threshold 50
```

ap dot11 24ghz cleanair alarm device

To configure the alarm for the 2.4-GHz devices, use the **ap dot11 24ghz cleanair alarm device** command.

ap dot11 24ghz cleanair alarm device [**bt-discovery**| **bt-link**| **canopy**| **cont-tx**| **dect-like**| **inv**| **jammer**| **nonstd**| **superag**| **tdd-tx**| **video**| **wimax-fixed**| **wimax-mobile**| **xbox**| **zigbee**]

Syntax Description

alarm	Configure 2.4 GHz cleanair alarms.
device	Configures the 2.4 GHz cleanair interference devices alarm.
bt-discovery	Bluetooth Discovery.
bt-link	Bluetooth Link.
canopy	Canopy devices.
cont-tx	Continuous Transmitter.
dect-like	Digital Enhanced Cordless Communication (DECT) like phone.
fh	802.11 frequency hopping devices.
inv	Devices using spectrally inverted Wi-Fi signals.
jammer	Jammer.
nonstd	Devices using nonstandard Wi-Fi channels.
superag	802.11 SuperAG devices.
tdd-tx	TDD Transmitter.
video	Video cameras.
wimax-fixed	WiMax Fixed.
wimax-mobile	WiMax Mobile
xbox	Xbox.
zigbee	802.15.4 devices.

Command Default

Disabled

Command Modes

Global configuration.

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Enable CleanAir first to be able to use the other commands within it.

Examples

This example shows how to enable the alarm to notify interferences from a zigbee device.

```
Controller(config)#ap dot11 24ghz cleanair alarm device zigbee
```

ap dot11 24ghz cleanair device

To configure the 2.4-GHz interference devices to report to the controller, use the **ap dot11 24ghz cleanair device** command.

ap dot11 24ghz cleanair device {**bt-discovery**| **bt-link**| **canopy**| **cont-tx**| **dect-like**| **inv**| **jammer**| **nonstd**| **superag**| **tdd-tx**| **video**| **wimax-fixed**| **wimax-mobile**| **xbox**| **zigbee**}

Syntax Description

bt-discovery	Bluetooth Discovery.
bt-link	Bluetooth Link.
canopy	Canopy devices.
cont-tx	Continuous Transmitter.
dect-like	Digital Enhanced Cordless Communication (DECT) like phone.
fh	802.11 frequency hopping devices.
inv	Devices using spectrally inverted Wi-Fi signals.
jammer	Jammer.
nonstd	Devices using nonstandard Wi-Fi channels.
superag	802.11 SuperAG devices.
tdd-tx	TDD Transmitter.
video	Video cameras.
wimax-fixed	WiMax Fixed.
wimax-mobile	WiMax Mobile
xbox	Xbox.
zigbee	802.15.4 devices.

Command Default

Disabled

Command Modes

Global configuration.

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Enable CleanAir first to be able to use the other commands within it.

Examples

This example shows how to enable CleanAir to report when a video camera interferes.

```
Controller(config)#ap dot11 24ghz cleanair device video
```

ap dot11 24ghz rrm channel cleanair-event

To enable EDRRM for 2.4 GHz devices, use the **ap dot11 24ghz rrm channel cleanair-event** command. To disable EDRRM, use the **no** form of the command.

ap dot11 24ghz rrm channel cleanair-event sensitivity {**high**| **low**| **medium**}

no ap dot11 24ghz rrm channel cleanair-event sensitivity {**high**| **low**| **medium**}

Syntax Description

cleanair-event	Enables EDRRM cleanair event-driven RRM parameters

Command Default

None.

Command Modes

Interface configuration.

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

None.

Examples

This example shows how to set EDRRM sensitivity to low.

```
Controller#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)#ap dot11 24ghz rrm channel cleanair-event sensitivity low
```

ap dot11 24ghz rrm channel device

To configure persistent non Wi-Fi device avoidance in the 802.11b channel assignment, use the **ap dot11 24ghz rrm channel device** command. To disable persistent device avoidance, use the **no** form of the command.

ap dot11 24ghz rrm channel device

no ap dot11 24ghz rrm channel device

Syntax Description

device	Configures persistent non Wi-Fi device avoidance in the 802.11b channel assignment.

Command Default

None.

Command Modes

Interface configuration.

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

None.

Examples

This example shows how to enable PDA.

```
Controller#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)#ap dot11 24ghz rrm channel device
```

ap dot11 5ghz cleanair

To enable CleanAir for detecting 5GHz devices, use the **ap dot11 5ghz cleanair** command.

ap dot11 5ghz cleanair

Command Default

Disabled

Command Modes

Global configuration.

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Enable CleanAir first to be able to use the other commands within it.

Examples

This example shows how to enable CleanAir for 5 -GHz devices.

```
Controller(config)#ap dot11 5ghz cleanair
```

ap dot11 5ghz cleanair alarm air-quality

To configure the alarm for the threshold value of air-quality for all 5-GHz devices, use the **ap dot11 5ghz cleanair alarm air-quality** command.

ap dot11 5ghz cleanair alarm air-quality threshold *threshold _value*

Syntax Description

air-quality	Configures the alarm for the air-quality of 5 GHz devices.
threshold *threshold _value*	Configures the threshold value for air-quality.

Command Default

Disabled

Command Modes

Global configuration.

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Enable CleanAir first to be able to use the other commands within it.

Examples

This example shows how to set the threshold value for the air-quality.

```
Controller(config)#ap dot11 5ghz cleanair alarm air-quality threshold 30
```

ap dot11 5ghz cleanair alarm device

To configure the alarm for the 5-GHz devices, use the **ap dot11 5ghz cleanair alarm device** command.

ap dot11 5ghz cleanair alarm device [**canopy**| **cont-tx**| **dect-like**| **inv**| **jammer**| **nonstd**| **radar**| **superag**| **tdd-tx**| **video**| **wimax-fixed**| **wimax-mobile**]

Syntax Description

alarm	Configure 2.4 GHz cleanair alarms.
device	Configures the 2.4 GHz cleanair interference devices alarm.
canopy	Canopy devices.
cont-tx	Continuous Transmitter.
dect-like	Digital Enhanced Cordless Communication (DECT) like phone.
inv	Devices using spectrally inverted Wi-Fi signals.
jammer	Jammer.
nonstd	Devices using nonstandard Wi-Fi channels.
radar	Radars.
superag	802.11 SuperAG devices.
tdd-tx	TDD Transmitter.
video	Video cameras.
wimax-fixed	WiMax Fixed.
wimax-mobile	WiMax Mobile

Command Default

Disabled

Command Modes

Global configuration.

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines Enable CleanAir first to be able to use the other commands within it.

Examples This example shows how to enable the alarm to notify interferences from a radar device.

```
Controller(config)#ap dot11 5ghz cleanair alarm device radar
```

ap dot11 5ghz cleanair device

To configure the 5-GHz interference devices to report to the controller, use the **ap dot11 5ghz cleanair device** command.

ap dot11 5ghz cleanair device {**canopy**| **cont-tx**| **dect-like**| **inv**| **jammer**| **nonstd**| **radar**| **superag**| **tdd-tx**| **video**| **wimax-fixed**| **wimax-mobile**}

Syntax Description

canopy	Canopy devices.
cont-tx	Continuous Transmitter.
dect-like	Digital Enhanced Cordless Communication (DECT) like phone.
inv	Devices using spectrally inverted Wi-Fi signals.
jammer	Jammer.
nonstd	Devices using nonstandard Wi-Fi channels.
radar	Radar.
superag	802.11 SuperAG devices.
tdd-tx	TDD Transmitter.
video	Video cameras.
wimax-fixed	WiMax Fixed.
wimax-mobile	WiMax Mobile

Command Default

Disabled

Command Modes

Global configuration.

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Enable CleanAir first to be able to use the other commands within it.

Examples This example shows how to enable CleanAir to report when a video camera interferes.

```
Controller(config)#ap dot11 5ghz cleanair device video
```

ap dot11 5ghz rrm channel cleanair-event

To enable EDRRM for 5-GHz devices, use the **ap dot11 5ghz rrm channel cleanair-event** command. To disable EDRRM, use the **no** form of the command.

ap dot11 5ghz rrm channel cleanair-event sensitivity {**high**| **low**| **medium**}

no ap dot11 5ghz rrm channel cleanair-event sensitivity {**high**| **low**| **medium**}

Syntax Description

cleanair-event	Enables EDRRM cleanair event-driven RRM parameters

Command Default

None.

Command Modes

Interface configuration.

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

None.

Examples

This example shows how to set the EDRRM sensitivity to high.

```
Controller#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)#ap dot11 5ghz rrm channel cleanair-event sensitivity high
```

ap dot11 5ghz rrm channel device

To configure persistent non Wi-Fi device avoidance in the 802.11a channel assignment, , use the **ap dot11 5ghz rrm channel device** command. To disable PDA, use the **no** form of the command.

ap dot11 5ghz rrm channel device

no ap dot11 5ghz rrm channel device

Syntax Description

cleanair-event	Configures persistent non Wi-Fi device avoidance in the 802.11a channel assignment.

Command Default

None.

Command Modes

Interface configuration.

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

None.

Examples

This example shows how to enable PDA for 802.11a devices.

```
Controller#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)#ap dot11 5ghz rrm channel device
```

show ap dot11 24ghz cleanair device type

To display the 2.4 GHz interference devices, use the **show ap dot11 24ghz cleanair device type** command.

show ap dot11 24ghz cleanair device type {**all**| **bt-discovery**| **bt-link**| **canopy**| **cont-tx**| **dect-like**| **fn**| **inv**| **jammer**| **mv-oven**| **nonstd**| **persistent**| **superag**| **tdd-tx**| **video**| **winmax-fixed**| **wimax-mobile**| **xbox**| **zigbee**}

Syntax Description

all	Displays all CleanAir Interferers for 2.4GHz band.
bt-discovery	Displays CleanAir Interferers of type BT Discovery for 2.4GHz band.
bt-link	Displays CleanAir Interferers of type BT Link for 2.4GHz band.
canopy	Displays CleanAir Interferers of type Canopy for 2.4GHz band.
cont-tx	Displays CleanAir Interferers of type Continuous TX for 2.4GHz band.
dect-like	Displays CleanAir Interferers of type DECT Like for 2.4GHz band.
fh	Displays CleanAir Interferers of type 802.11FH for 2.4GHz band.
inv	Displays CleanAir Interferers of type WiFi Inverted for 2.4GHz band.
jammer	Displays CleanAir Interferers of type Jammer for 2.4GHz band.
mv-oven	Displays CleanAir Interferers of type MW Oven for 2.4GHz band.
nonstd	Displays CleanAir Interferers of type WiFi Inv. Ch for 2.4GHz band.
persistent	Displays CleanAir Interferers of type Persistent for 2.4GHz band.
superag	Displays CleanAir Interferers of type SuperAG for 2.4GHz band.
tdd-tx	Displays CleanAir Interferers of type TDD Transmit for 2.4GHz band.
video	Displays CleanAir Interferers of type Video Camera for 2.4GHz band.
winmax-fixed	Displays CleanAir Interferers of type WiMax Fixed for 2.4GHz band.
wimax-mobile	Displays CleanAir Interferers of type WiMax Mobile for 2.4GHz band.
xbox	Displays CleanAir Interferers of type Xbox for 2.4GHz band.
zigbee	Displays CleanAir Interferers of type zigbee for 2.4GHz band.

Command Default

None.

Command Modes Global configuration.

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines Interference devices will be listed only if there is an interference from any 2.4-GHz devices.

Examples This example shows how to view all the 2.4-GHz interference devices.

```
Controller#show ap dot11 24ghz cleanair device type all

DC    = Duty Cycle (%)
ISI   = Interference Severity Index (1-Low Interference, 100-High Interference)
RSSI  = Received Signal Strength Index (dBm)
DevID = Device ID

No    ClusterID          DevID  Type           AP Name                 ISI  RSSI  DC
Channel
-------------------------------------------------------------------------------------------------
```

show ap dot11 5ghz cleanair device type

To display the 5 GHz interference devices, use the **show ap dot11 5ghz cleanair device type** command.

show ap dot11 5ghz cleanair device type {**all**| **canopy**| **cont-tx**| **dect-like**| **inv**| **jammer**| **nonstd**| **persisten**| **superag**| **tdd-tx**| **video**| **wimax-fixed**| **wimax-mobile**}

Syntax Description

all	Displays all CleanAir Interferers for 2.4GHz band.
canopy	Displays CleanAir Interferers of type Canopy for 2.4GHz band.
cont-tx	Displays CleanAir Interferers of type Continuous TX for 2.4GHz band.
dect-like	Displays CleanAir Interferers of type DECT Like for 2.4GHz band.
inv	Displays CleanAir Interferers of type WiFi Inverted for 2.4GHz band.
jammer	Displays CleanAir Interferers of type Jammer for 2.4GHz band.
nonstd	Displays CleanAir Interferers of type WiFi Inv. Ch for 2.4GHz band.
persistent	Displays CleanAir Interferers of type Persistent for 2.4GHz band.
superag	Displays CleanAir Interferers of type SuperAG for 2.4GHz band.
tdd-tx	Displays CleanAir Interferers of type TDD Transmit for 2.4GHz band.
video	Displays CleanAir Interferers of type Video Camera for 2.4GHz band.
winmax-fixed	Displays CleanAir Interferers of type WiMax Fixed for 2.4GHz band.
wimax-mobile	Displays CleanAir Interferers of type WiMax Mobile for 2.4GHz band.

Command Default

None

Command Modes

Global configuration.

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Interference devices will be listed only if there is an interference from any 5 GHz devices.

Examples

This example shows how to view all the 5 GHz interference devices.

```
Controller#show ap dot11 5ghz cleanair device type all

DC    = Duty Cycle (%)
ISI   = Interference Severity Index (1-Low Interference, 100-High Interference)
RSSI  = Received Signal Strength Index (dBm)
DevID = Device ID

No    ClusterID          DevID  Type           AP Name                 ISI  RSSI  DC
Channel
-------------------------------------------------------------------------------------------
```

PART XIII

Mobility

Mobility Commands

mobility anchor

To configure and enable mobility sticky anchoring, use the **mobility anchor** sticky command. To disable the sticky anchoring, use the **no** form of the command.

To configure guest anchoring, use **mobility anchor** ip

. To delete the guest anchor, use the **no** form of the command.

mobility anchor {**sticky** | *ip-addr* }

no mobility anchor {**sticky** | *ip-addr* }

Syntax Description

sticky	The client is anchored to the first switch that it associates. **Note** This command is by default enabled and ensures low roaming latency. This ensures that the point of presence for the client does not change when the client joins the mobility domain and roams within the domain.
ip-addr	Configures the IP address for guest anchor controller.

Command Default

None.

Command Modes

WLAN Configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

- The wlan_id or guest_lan_id must exist and be disabled.
- Auto-anchor mobility is enabled for the WLAN or wired guest LAN when you configure the first mobility anchor.
- Deleting the last anchor disables the auto-anchor mobility feature and resumes normal mobility for new associations.
- Mobility uses the following ports, that are allowed through the firewall:
  - 16666
  - 16667
  - 16668

Examples This example shows how to enable the sticky mobility anchor:

```
Controller(config-wlan)# mobility anchor sticky
```

Examples This example shows how to configure guest anchoring:

```
Controller (config-wlan)# mobility anchor <ip>
```

wireless mobility

To configure the inter-switch mobility manager, use the **wireless mobility** command.

wireless mobility {**dscp** *value* }

Syntax Description

dscp *value*	Configures the Mobility inter controller DSCP value.

Command Default

None.

Command Modes

Global Configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shoes how to configure mobility inter controller DSCP with an value of 20:

```
Controller(config)# wireless mobility dscp 20
```

wireless mobility controller

To configure mobility controller settings, use the **wireless mobility controller** command. To remove a mobility controller settings, use the **no** form of the command.

wireless mobility controller peer-group *peer-group-name* [**bidge-domain-id** *id* | **member ip** *ip-address* [**public-ip** | *public-ip-address*]| **multicast ip** *multicast-address*]

nowireless mobility controller peer-group *peer-group-name* [**bidge-domain-id** *id* | **member ip** *ip-address* [**public-ip** | *public-ip-address*]| **multicast ip** *multicast-address*]

Syntax Description

peer-group *peer-group-name*	Creates a mobility peer group.
bidge-domain-id *id*	Configures bridge domain ID for the mobility peer group.
member ip *ip-address* **public-ip** *public-ip-address*	Adds or deletes a peer group member. **Note** The **public-ip** *public-ip-address* is optional and is only when the mobility peer is NATed.
multicast ip *multicast-address*	Configures multicast settings of a peer group.

Command Default

None.

Command Modes

Global Configuration.

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

In the Converged Access solution, WLANs are mapped to VLANs, and VLANs are usually mapped to subnets. For seamless roaming, the same VLAN configured on two controllers is expected to be mapped to the same subnet. This identical mapping from one controller to the next is important for roaming, because the controllers taking care of the roaming event need to determine if they need:

- To address a Layer 2 roaming event (when WLAN to VLAN and subnet mapping are identical on the anchor and the foreign controller), or
- a Layer 3 roaming event (when WLAN to VLAN and subnet mapping are different between the anchor and the foreign controller).

This determination is made by comparing the WLAN SSID string and the VLAN ID between controllers. In cases where the WLAN SSID and VLAN ID are identical, the expectation is that the subnet associated to the VLAN is identical as well.

There may be cases where this mapping is not identical. For example, suppose that WLAN1 on controller 1 is mapped to VLAN 14, and that VLAN 14 on controller1 is mapped to the subnet 10.10.14.0/24. Also suppose that WLAN 1 on controller 2 is mapped to VLAN 14, but that VLAN 14 on controller 2 is mapped to this subnet 172.31.24.0/24. Controllers 1 and 2 will compare WLAN1 and the associated VLAN and conclude that they are addressing a Layer 2 roaming event, whereas the roaming even is Layer 3, as VLAN 14 does not have the same Layer 3 significance on both controllers.

When this disconnect between VLANs and their associated subnet occurs, you may want to configure your Converged Access controllers for different bridge domain IDs. Two controllers in the same bridge domain ID are expected to have the same VLAN to subnet mapping. Cisco recommends that you configure the same bridge domain ID on all controllers that share the same VLAN to subnet mapping, and between which roaming is expected.

Examples This example shows how to configure a controller bridge domain ID.

```
Controller (config)# wireless mobility controller peer-group SPG1 bridge-domain-id 111
```

Examples This example shows how to create and configure a controller peer group with a bridge ID of 111:

```
Controller(config)# controller peer-group TestDocPeerGroup bridge-domain-id 111
```

Examples This example shows how to disable a controller peer group with a bridge ID of 111:

```
Controller(config)# no controller peer-group TestDocPeerGroup bridge-domain-id 111
```

Examples This examples shows the configuration for a NATed member (the IP 172.19.13.15 is outside the NAT):

```
Controller (config)# wireless mobility group ip 1.4.91.2 public-ip 172.19.13.15
```

Examples This examples shows the configuration of a member when it is not NATed (the IP 1.4.91.2 is inside the NAT):

```
Controller (config)# wireless mobility group ip 1.4.91.2
```

wireless mobility group keepalive

To configure the mobility group parameter and keep alive its ping parameters, use the **wireless mobility group keepalive** command. To remove a mobility group parameter, use the no form of the command.

wireless mobility group keepalive {**count** *number* | **interval** *interval* }

no wireless mobility group keepalive {**count** *numbe r*| **interval** *interval* }

Syntax Description

count *number*	Number of times that a ping request is sent to a mobility group member before the member is considered unreachable. The range is from 3 to 20. The default is 3.
interval *interval*	Interval of time between each ping request sent to a mobility group member. The range is from 1 to 30 seconds. The default value is 10 seconds.

Command Default

3 seconds for count and 10 seconds for interval.

Command Modes

Global Configuration.

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The default values for *interval* is ten seconds and the default for *retries* is set to three.

Examples

This example shows how to specify the amount of time between each ping request sent to a mobility group member to 10 seconds:

```
Controller(config)# wireless mobility group keepalive count 10
```

wireless mobility group member ip

To add or delete users from mobility group member list, use the **wireless mobility group member ip** command. To remove a member from the mobility group, use the **no** form of the command.

wireless mobility group member ip *ip-address* [**public-ip** *public-ip-address*] [**group** *group-name*]

no wireless mobility group member ip *ip-address*

Syntax Description

ip-address	The IP address of the member controller.
public-ip *public-ip-address*	(Optional) Member controller public IP address. **Note** This command is used only when the member is behind a NAT. Only static IP NAT is supported.
group *group-name*	(Optional) Member controller group name. **Note** This command is used only when the member added in not in the same group as the local mobility controller.

Command Default

None.

Command Modes

Global Configuration.

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The mobility group is used when there is more than one Mobility Controller (MC) in a given deployment. The mobility group can be assigned with a name or it can use the default group name. The mobility group members need to be configured on all the members of the group to roam within the group.

Examples

This example shows how to add a member in a mobility group:

```
Controller(config)# mobility group member ip 10.104.171.101 group TestDocGroup
```

wireless mobility group name

To configure hte mobility domain name, use the **wireless mobility group name** command. To remove the mobility domain name, use the **no** form of the command.

Note If you are configuring the mobility group in a network where network address translation (NAT) is enabled, enter the IP address that is sent to the controller from the NAT device rather than the controller's management interface IP address. Otherwise, mobility will fail among controllers in the mobility group.

wireless mobility group name *domain-name*

no wireless mobility group name

Syntax Description

domain-name	Creates a mobility group by entering this command. The domain name can be up to 31 case-sensitive characters.

Command Default

Default.

Command Modes

Global Configuration.

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to configure a mobility domain name lab1:

```
Controller(config)# mobility group domain lab1
```

wireless mobility oracle ip

To configure mobility oracle settings, use the **wireless mobility oracle ip** command. To remove the mobility oracle settings, use the **no** form of the command.

To enable or disable the **mobility oracle** functionality, use the **no** form of the command.

wireless mobility oracle ip *mo-ip-address*

no wireless mobility oracle ip *mo-ip-address*

no wireless mobility oracle

Syntax Description

mo-ip-address	Defines IP address of mobility oracle.

Command Default

None.

Command Modes

Global Configuration.

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

By default the **[no] wireless mobility oracle** is configured on the controller. A peer mobility controller must be configured for mobility to work.

The mobility oracle is recommended when more than one mobility controller (MC) in a configurtion is allowed a fast client join and roaming across the sub-domains. The mobility oracle (MO) must be enabled on one of the MCs and the remaing MCs in the sub-domain must point to that MO.

Examples

This example shows how to configure the mobility oracle.

```
Controller(config)# wireless mobility oracle ip 10.104.171.102
```

show wireless mobility

To view the wireless mobility summary, use the **show wireless mobility** command.

show wireless mobility [**agent** | *mobility-agent-ip* **| client summary | ap-list | controller client summary| dtls connections| oracle summary | statistics summary**]

Syntax Description

agent *mobility-agent-ip* **client summary**	Shows the active clients on a mobility agent.
ap-list	Shows the list of Cisco APs known to the mobility group.
controller client summary	Shows the active clients in the subdomain.
dtls connections	Shows the DTLS server status.
oracle summary	Displays the status of the mobility-controllers known to the mobility-oracle.
mobilityoracleclient summary	Shows the mobility-oracle client and status database.
statistics	Shows the statistics for the Mobility manager.
summary	Shows the summary of the mobility manager.

Command Default

None

Command Modes

Global Configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to display a summary of the mobility manager:

```
Controller (config)# show wireless mobility ap-list

AP name                              AP radio MAC      Controller IP     Learnt from
-------------------------------------------------------------------------------------------------
TSIM_AP-101                          0000.2000.6600    9.9.9.2           Self
TSIM_AP-102                          0000.2000.6700    9.9.9.2           Self
TSIM_AP-103                          0000.2000.6800    9.9.9.2           Self
TSIM_AP-400                          0000.2001.9100    9.9.9.2           Self
TSIM_AP-402                          0000.2001.9300    9.9.9.2           Self
TSIM_AP-403                          0000.2001.9400    9.9.9.2           Self
TSIM_AP-406                          0000.2001.9700    9.9.9.2           Self
TSIM_AP-407                          0000.2001.9800    9.9.9.2           Self
```

```
TSIM_AP-409                     0000.2001.9a00     9.9.9.2          Self
```

clear wireless mobility statistics

To clear wireless statisitcs, use the **clear wireless mobility statistic s** command.

clear wireless mobility statistics

Command Default None.

Command Modes Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines You can clear all the information by using the **clear wireless mobility statistics** command.

Examples This example shows how to clear wireless mobility statistics:

```
Controller (confog)# clear wireless mobility statistics
```

PART XIV

IPv6

IPv6 Commands

ipv6 flow monitor

This command activates a previously created flow monitor by assigning it to the interface to analyze incoming or outgoing traffic.

To activate a previously created flow monitor, use the **ipv6 flow monitor** command. To de-activate a flow monitor, use the **no** form of the command.

ipv6 flow monitor *ipv6-monitor-name* [**sampler** *ipv6-sampler-name*] {**input**| **output**}

no ipv6 flow monitor *ipv6-monitor-name* [**sampler** *ipv6-sampler-name*] {**input**| **output**}

Syntax Description

ipv6-monitor-name	Activates a previously created flow monitor by assigning it to the interface to analyze incoming or outgoing traffic.
sampler *ipv6-sampler-name*	Applies the flow monitor sampler.
input	Applies the flow monitor on input traffic.
output	Applies the flow monitor on output traffic.

Command Default

IPv6 flow monitor is not activated until it is assigned to an interface.

Command Modes

Interface Configuration.

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You cannot attach a NetFlow monitor to a port channel interface. If both service module interfaces are part of an EtherChannel, you should attach the monitor to both physical interfaces.

Examples

This example shows how to apply a flow monitor to an interface:

```
Controller(config)# interface gigabitethernet 1/1/2
Controller(config-if)# ip flow monitor FLOW-MONITOR-1 input
Controller(config-if)# ip flow monitor FLOW-MONITOR-2 output
Controller(config-if)# end
```

ipv6 traffic-filter

This command enables IPv6 traffic filter.

To enable the filtering of IPv6 traffic on an interface, use the **ipv6 traffic-filter** command. To disable the filtering of IPv6 traffic on an interface, use the **no** form of the command.

Use the **ipv6 traffic-filter** interface configuration command on the switch stack or on a standalone switch to filter IPv6 traffic on an interface. The type and direction of traffic that you can filter depends on the feature set running on the switch stack. Use the **no** form of this command to disable the filtering of IPv6 traffic on an interface.

ipv6 traffic-filter [web] *acl-name*

no ipv6 traffic-filter [web]

Syntax Description

web	(Optional) Specifies an IPv6 access name for the WLAN Web ACL.
acl-name	Specifies an IPv6 access name.

Command Default

Filtering of IPv6 traffic on an interface is not configured.

Command Modes

wlan

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

To configure the dual IPv4 and IPv6 template, enter the **sdm prefer dual-ipv4-and-ipv6 {default | vlan}** global configuration command and reload the switch.

You can use the **ipv6 traffic-filter** command on physical interfaces (Layer 2 or Layer 3 ports), Layer 3 port channels, or switch virtual interfaces (SVIs).

You can apply an ACL to outbound or inbound traffic on Layer 3 interfaces (port ACLs), or to inbound traffic on Layer 2 interfaces (router ACLs).

If **any** port ACL (IPv4, IPv6, or MAC) is applied to an interface, that port ACL is used to filter packets, and any router ACLs attached to the SVI of the port VLAN are ignored.

Examples

This example shows how to filter IPv6 traffic on an interface:

```
Controller(config-wlan)# ipv6 traffic-filter TestDocTrafficFilter
```

show wireless ipv6 statistics

This command is used to display the IPv6 packet counter statistics.

To view IPv6 packet counter statistics, use the **show wireless ipv6 statistics** command.

show wireless ipv6 statistics

Command Default

None.

Command Modes

User EXEC.

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

The following example shows the summary of the IPv6 packet counter statistics:

```
Controller# show wireless ipv6 statistics
NS Forwarding to wireless clients               : Enabled

RS count                                        : 0
RA count                                        : 0
NS count                                        : 0
NA count                                        : 0
Other NDP packet count                          : 0
-----------------------------------------------------
Non-IPv6 packets count                          : 0
Non-IPv6 Multicast Destination MAC packet count : 0
Invalid length packets count                    : 0
Null packets count                              : 0
Invalid Source MAC packets count                : 0
-----------------------------------------------------
TCP packets count                               : 0
UDP packets count                               : 0
Fragmented packets count                        : 0
No next header packets count                    : 0
Other type packets count                        : 0
-----------------------------------------------------
Total packets count                             : 0
-----------------------------------------------------
Blocked RA packets count                        : 0
Blocked NS packets count                        : 0
```

PART XV

Flexible Netflow

Flexible NetFlow Command Reference

This chapter contains the Flexible NetFlow-related commands:

cache

To configure a flow cache parameter for a flow monitor, use the **cache** command in flow monitor configuration mode. To remove a flow cache parameter for a flow monitor, use the **no** form of this command.

cache {**timeout** {**active| inactive**} *seconds*| **type normal**}

no cache {**timeout** {**active| inactive**} | **type**}

Syntax Description

timeout	Specifies the flow timeout.
active	Specifies the active flow timeout.
inactive	Specifies the inactive flow timeout.
seconds	The timeout value in seconds. The range is 1 to 604800 (7 days).
type	Specifies the type of the flow cache.
normal	Configures a normal cache type. The entries in the flow cache will be aged out according to the **timeout active** *seconds* and **timeout inactive** *seconds* settings. This is the default cache type.

Command Default

The default flow monitor flow cache parameters are used.

The following flow cache parameters for a flow monitor are enabled:

- Cache type: normal
- Active flow timeout: 1800 seconds
- Inactive flow timeout: 15 seconds

Command Modes

Flow monitor configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Each flow monitor has a cache that it uses to store all the flows it monitors. Each cache has various configurable elements, such as the time that a flow is allowed to remain in it. When a flow times out, it is removed from the cache and sent to any exporters that are configured for the corresponding flow monitor.

If a cache is already active (that is, you have applied the flow monitor to at least one interface in the controller), your changes to the parameters will not take effect until you either reboot the controller or remove the flow monitor from every interface and then reapply it. Therefore, whenever possible you should customize the parameters for the cache before you apply the flow monitor to an interface. You can modify the timers, flow exporters, and statistics parameters for a cache while the cache is active.

The **cache timeout active** command controls the aging behavior of the normal type of cache. If a flow has been active for a long time, it is usually desirable to age it out (starting a new flow for any subsequent packets in the flow). This age out process allows the monitoring application that is receiving the exports to remain up to date. By default, this timeout is 1800 seconds (30 minutes), but it can be adjusted according to system requirements. A larger value ensures that long-lived flows are accounted for in a single flow record; a smaller value results in a shorter delay between starting a new long-lived flow and exporting some data for it.

The **cache timeout inactive** command also controls the aging behavior of the normal type of cache. If a flow has not seen any activity for a specified amount of time, that flow will be aged out. By default, this timeout is 15 seconds, but this value can be adjusted depending on the type of traffic expected. If a large number of short-lived flows is consuming many cache entries, reducing the inactive timeout can reduce this overhead. If a large number of flows frequently get aged out before they have finished collecting their data, increasing this timeout can result in better flow correlation.

The **cache type normal** command specifies the normal cache type. This is the default cache type. The entries in the cache will be aged out according to the **timeout active** *seconds* and **timeout inactive** *seconds* settings. When a cache entry is aged out, it is removed from the cache and exported via any exporters configured for the monitor associated with the cache.

Note When a cache becomes full, new flows will not be monitored.

Examples

The following example shows how to configure the active timeout for the flow monitor cache:

```
Controller(config)# flow monitor FLOW-MONITOR-1
Controller(config-flow-monitor)# cache timeout active 4800
```

The following example shows how to configure the inactive timer for the flow monitor cache:

```
Controller(config)# flow monitor FLOW-MONITOR-1
Controller(config-flow-monitor)# cache timeout inactive 30
```

The following example shows how to configure a normal cache:

```
Controller(config)# flow monitor FLOW-MONITOR-1
Controller(config-flow-monitor)# cache type normal
```

collect counter

To configure the number of bytes or packets in a flow as a non-key field for a flow record, use the **collect counter** command in flow record configuration mode. To disable the use of the number of bytes or packets in a flow (counters) as a non-key field for a flow record, use the **no** form of this command.

collect counter {**bytes** {**layer2 long**| **long**}| **packets long**}

no collect counter {**bytes** {**layer2 long**| **long**}| **packets long**}

Syntax Description

bytes	Configures the number of bytes seen in a flow as a non-key field and enables collecting the total number of bytes from the flow.
layer2 long	Enables collecting the total number of Layer 2 bytes or packets from the flow using a 64-bit counter.
long	Enables collecting the total number of bytes or packets from the flow using a 64-bit counter.
packets long	Configures the number of packets seen in a flow as a non-key field and enables collecting the total number of packets from the flow using a 64-bit counter.

Command Default

The number of bytes or packets in a flow is not configured as a non-key field.

Command Modes

Flow record configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The Flexible NetFlow **collect** commands are used to configure non-key fields for the flow monitor record and to enable capturing the values in the fields for the flow created with the record. The values in non-key fields are added to flows to provide additional information about the traffic in the flows. A change in the value of a non-key field does not create a new flow. In most cases, the values for non-key fields are taken from only the first packet in the flow.

The **collect counter bytes long** command configures a 64-bit counter for the number of bytes seen in a flow.

The **collect counter packets long** command configures a 64-bit counter that will be incremented for each packet seen in the flow. It is unlikely that a 64-bit counter will ever restart at 0.

Examples

The following example configures the total number of bytes in the flows as a non-key field:

```
Controller(config)# flow record FLOW-RECORD-1
Controller(config-flow-record)#collect counter bytes long
```

The following example configures the total number of packets from the flows as a non-key field:

```
Controller(config)# flow record FLOW-RECORD-1
Controller(config-flow-record)# collect counter packets long
```

collect interface

To configure the input interface as a non-key field for a flow record, use the **collect interface** command in flow record configuration mode. To disable the use of the input and output interface as a non-key field for a flow record, use the **no** form of this command.

collect interface input

no collect interface input

Syntax Description

input	Configures the input interface as a non-key field and enables collecting the input interface from the flows.

Command Default

The input interface is not configured as a non-key field.

Command Modes

Flow record configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The Flexible NetFlow **collect** commands are used to configure non-key fields for the flow monitor record and to enable capturing the values in the fields for the flow created with the record. The values in non-key fields are added to flows to provide additional information about the traffic in the flows. A change in the value of a non-key field does not create a new flow. In most cases, the values for non-key fields are taken from only the first packet in the flow.

Examples

The following example configures the input interface as a non-key field:

```
Controller(config)# flow record FLOW-RECORD-1
Controller(config-flow-record)# collect interface input
```

collect timestamp absolute

To configure the absolute time of the first seen or last seen packet in a flow as a non-key field for a flow record, use the **collect timestamp absolute** command in flow record configuration mode. To disable the use of the first seen or last seen packet in a flow as a non-key field for a flow record, use the **no** form of this command.

collect timestamp absolute {**first**| **last**}

no collect timestamp absolute {**first**| **last**}

Syntax Description

first	Configures the absolute time for the time that the first packet was seen from the flows as a non-key field and enables collecting time stamps based on the absolute time for the time the first packet was seen from the flows.
last	Configures the absolute time for the time that the last packet was seen from the flows as a non-key field and enables collecting time stamps based on the absolute time for the time that the most recent packet was seen from the flows.

Command Default

The absolute time field is not configured as a non-key field.

Command Modes

Flow record configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The Flexible NetFlow **collect** commands are used to configure non-key fields for the flow monitor record and to enable capturing of the values in the fields for the flow created with the record. The values in non-key fields are added to flows to provide additional information about the traffic in the flows. A change in the value of a non-key field does not create a new flow. In most cases, the values for non-key fields are taken from only the first packet in the flow.

Examples

The following example configures time stamps based on the absolute time for the time that the first packet was seen from the flows as a non-key field:

```
Controller(config)# flow record FLOW-RECORD-1
Controller(config-flow-record)# collect timestamp absolute first
```

The following example configures the time stamps based on the absolute time for the time that the most recent packet was seen from the flows as a non-key field:

```
Controller(config)# flow record FLOW-RECORD-1
Controller(config-flow-record)# collect timestamp absolute last
```

collect transport tcp flags

To enable the collecting of transport TCP flags from a flow record, use the **collect transport tcp flags** command in flow record configuration mode. To disable the collecting of transport TCP flags from the flow, use the **no** form of this command.

collect transport tcp flags

no collect transport tcp flags

Syntax Description

This command has no keywords or arguments.

Command Default

The transport layer fields are not configured as a non-key field.

Command Modes

Flow record configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The Flexible NetFlow **collect** commands are used to configure non-key fields for the flow monitor record and to enable capturing the values in the fields for the flow created with the record. The values in non-key fields are added to flows to provide additional information about the traffic in the flows. A change in the value of a non-key field does not create a new flow. In most cases, the values for non-key fields are taken from only the first packet in the flow.

Examples

The following example collects the TCP flags from the specified flow record:

```
Controller(config)# flow record FLOW-RECORD-1
Controller(config-flow-record)# collect transport tcp flags
```

datalink flow monitor (wireless)

To enable NetFlow monitoring in a WLAN, use the **datalink flow monitor** command in WLAN configuration mode. To disable NetFlow monitoring, use the **no** form of this command.

datalink flow monitor *datalink-monitor-name*{**input | output**}

no datalink flow monitor *datalink-monitor-name*{**input | output**}

Syntax Description

datalink-monitor-name	Flow monitor name. The name is case sensitive and consists of alphanumeric characters, with a maximum of 31 characters.
input	Specifies the NetFlow monitor for ingress traffic.
output	Specifies the NetFlow monitor for egress traffic.

Command Default

Flow monitor is not configured by default for WLAN interface.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Before you apply a flow monitor to an interface with the **datalink flow monitor** command, you must have already created the flow monitor using the **flow monitor** global configuration command.

Examples

This example shows how to enable NetFlow monitoring on a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# datalink flow monitor test output
Controller(config-wlan)# end
```

This example shows how to disable NetFlow monitor on a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# no datalink flow monitor test output
Controller(config-wlan)# end
```

default

To configure the default values for a Flexible NetFlow (FNF) flow exporter, use the **default** command in flow exporter configuration mode.

default {**description**| **destination**| **dcsp**| **export-protocol**| **option** {**exporter-stats**| **interface-table**| **sampler-table**}| **source**| **template data timeout**| **transport**| **ttl**}

Syntax Description

description	Provides a description for the flow exporter.
destination	Configures the export destination.
dscp	Configures optional Differentiated Services Code Point (DSCP) values.
export-protocol	Configures the export protocol version.
option	Selects the option for exporting.
exporter-stats	Selects the exporter statistics option.
interface-table	Selects the interface SNMP index-to-name table option.
sampler-table	Selects the interface export sampler table option.
source	Configures the originating interface.
template data timeout	Configures the flow exporter template to resend flow exporter data based on a timeout.
transport	Configures the transport protocol.
ttl	Configures optional time-to-live (TTL) or hop limit.

Command Modes

Flow exporter configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Use the **default** command to configure the default values for an FNF flow exporter. The flow exporter information is needed to export the data metrics to a specified destination, port number, and so on.

Examples

The following example shows how to set the default destination for an FNF flow exporter:

```
Controller(config)# flow exporter e1
Controller(config-flow-exporter)# default destination
```

description

To configure a description for a flow monitor, flow exporter, or flow record, use the **description** command in the appropriate configuration mode. To remove a description, use the **no** form of this command.

description *description*

no description *description*

Syntax Description

description	Text string that describes the flow monitor, flow exporter, or flow record.

Command Default

The default description for a flow sampler, flow monitor, flow exporter, or flow record is "User defined."

Command Modes

The following command modes are supported:

Flow exporter configuration

Flow monitor configuration

Flow record configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

The following example configures a description for a flow monitor:

```
Controller(config)# flow monitor FLOW-MONITOR-1
Controller(config-flow-monitor)# description Monitors traffic to 172.16.100.0 255.255.255.0
```

destination

To configure an export destination for a flow exporter, use the **destination** command in flow exporter configuration mode. To remove an export destination for a flow exporter, use the **no** form of this command.

destination {*hostname*| *ip-address*} [**vrf** *vrf-name*]

no destination {*hostname*| *ip-address*} [**vrf** *vrf-name*]

Syntax Description

hostname	Hostname of the device to which you want to send the NetFlow information.
ip-address	IP address of the workstation to which you want to send the NetFlow information.
vrf *vrf-name*	(Optional) Specifies that the export data packets are to be sent to the named Virtual Private Network (VPN) routing and forwarding (VRF) instance for routing to the destination, instead of to the global routing table.

Command Default

An export destination is not configured.

Command Modes

Flow exporter configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Each flow exporter can have only one destination address or hostname.

For some releases, you can export data to a destination using an IPv6 address.

When you configure a hostname instead of the IP address for the device, the hostname is resolved immediately and the IP address is stored in the running configuration. If the hostname-to-IP-address mapping that was used for the original Domain Name System (DNS) name resolution changes dynamically on the DNS server, the controller does not detect this, and the exported data continues to be sent to the original IP address, resulting in a loss of data. Resolving the hostname immediately is a prerequisite of the export protocol to ensure that the templates and options arrive before the data.

Examples

The following example shows how to configure the networking device to export the Flexible NetFlow cache entry to a destination system:

```
Controller(config)# flow exporter FLOW-EXPORTER-1
Controller(config-flow-exporter)# destination 10.0.0.4
```

The following example shows how to configure the networking device to export the Flexible NetFlow cache entry to a destination system using a VRF named VRF-1:

```
Controller(config)# flow exporter FLOW-EXPORTER-1
Controller(config-flow-exporter)# destination 172.16.10.2 vrf VRF-1
```

dscp

To configure a differentiated services code point (DSCP) value for flow exporter datagrams, use the **dscp** command in flow exporter configuration mode. To remove a DSCP value for flow exporter datagrams, use the **no** form of this command.

dscp *dscp*

no dscp *dscp*

Syntax Description

dscp	DSCP to be used in the DSCP field in exported datagrams. The range is 0 to 63. The default is 0.

Command Default

The differentiated services code point (DSCP) value is 0.

Command Modes

Flow exporter configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

None

Examples

The following example sets 22 as the value of the DSCP field in exported datagrams:

```
Controller(config)# flow exporter FLOW-EXPORTER-1
Controller(config-flow-exporter)# dscp 22
```

export-protocol netflow-v9

To configure NetFlow Version 9 export as the export protocol for a Flexible NetFlow exporter, use the **export-protocol netflow-v9** command in flow exporter configuration mode.

export-protocol netflow-v9

Syntax Description

This command has no keywords or arguments.

Command Default

NetFlow Version 9 is enabled.

Command Modes

Flow exporter configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The controller does not support NetFlow v5 export format, only NetFlow v9 export format is supported.

Examples

The following example configures NetFlow Version 9 export as the export protocol for a NetFlow exporter:

```
Controller(config)# flow exporter FLOW-EXPORTER-1
Controller(config-flow-exporter)# export-protocol netflow-v9
```

match datalink dot1q priority

To configure the 802.1Q (dot1q) priority value as a key field for a flow record, use the **match datalink dot1q priority** command in flow record configuration mode. To disable the use of the priority as a key field for a flow record, use the **no** form of this command.

match datalink dot1q priority

no match datalink dot1q priority

Syntax Description

This command has no keywords or arguments.

Command Default

The priority field is not configured as a key field.

Command Modes

Flow record configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The observation point of the **match datalink dot1q priority** command is the interface to which the flow monitor that contains the flow record with the command is applied.

Examples

The following example configures the 802.1Q priority as a key field for a flow record:

```
Controller(config)# flow record FLOW-RECORD-1
Controller(config-flow-record)# match datalink dot1q priority
```

match datalink dot1q vlan

To configure the 802.1Q (dot1q) VLAN value as a key field for a flow record, use the **match datalink dot1q vlan** command in flow record configuration mode. To disable the use of the 802.1Q VLAN value as a key field for a flow record, use the **no** form of this command.

match datalink dot1q vlan {**input**| **output**}

no match datalink dot1q vlan {**input**| **output**}

Syntax Description

input	Configures the VLAN ID of traffic being received by the controller as a key field.
output	Configures the VLAN ID of traffic being transmitted by the controller as a key field.

Command Default

The 802.1Q VLAN ID is not configured as a key field.

Command Modes

Flow record configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The input and output keywords of the **match datalink dot1q vlan** command are used to specify the observation point that is used by the **match datalink dot1q vlan** command to create flows based on the unique 802.1q VLAN IDs in the network traffic.

Examples

The following example configures the 802.1Q VLAN ID of traffic being received by the controller as a key field for a flow record:

```
Controller(config)# flow record FLOW-RECORD-1
Controller(config-flow-record)# match datalink dot1q vlan input
```

match datalink ethertype

To configure the Ethertype of the packet as a key field for a flow record, use the **match datalink ethertype** command in flow record configuration mode. To disable the Ethertype of the packet as a key field for a flow record, use the **no** form of this command.

match datalink ethertype

no match datalink ethertype

Syntax Description

This command has no keywords or arguments.

Command Default

The Ethertype of the packet is not configured as a key field.

Command Modes

Flow record configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The observation point of the **match datalink ethertype** command is the interface to which the flow monitor that contains the flow record with the command is applied.

Examples

The following example configures the Ethertype of the packet as a key field for a Flexible NetFlow flow record:

```
Controller(config)# flow record FLOW-RECORD-1
Controller(config-flow-record)# match datalink ethertype
```

match datalink mac

To configure the use of MAC addresses as a key field for a flow record, use the **match datalink mac** command in flow record configuration mode. To disable the use of MAC addresses as a key field for a flow record, use the **no** form of this command.

match datalink mac {**destination address input**| **source address input**}

no match datalink mac {**destination address input**| **source address input**}

Syntax Description

destination address	Configures the use of the destination MAC address as a key field.
input	Specifies the MAC address of input packets.
source address	Configures the use of the source MAC address as a key field.

Command Default

MAC addresses are not configured as a key field.

Command Modes

Flow record configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The **input** and **output** keywords of the **match datalink mac** command are used to specify the observation point that is used by the **match datalink mac** command to create flows based on the unique MAC addressees in the network traffic.

Examples

The following example configures the use of the destination MAC address of packets that are received by the controller as a key field for a flow record:

```
Controller(config)# flow record FLOW-RECORD-1
Controller(config-flow-record)# match datalink mac destination address input
```

match datalink vlan

To configure the VLAN ID as a key field for a flow record, use the **match datalink vlan** command in flow record configuration mode. To disable the use of the VLAN ID value as a key field for a flow record, use the **no** form of this command.

match datalink vlan input

no match datalink vlan input

Syntax Description

input	Configures the VLAN ID of traffic being received by the controller as a key field.

Command Default

The VLAN ID is not configured as a key field.

Command Modes

Flow record configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The **input** keyword is used to specify the observation point that is used by the **match datalink vlan** command to create flows based on the unique VLAN IDs in the network traffic.

Examples

The following example configures the VLAN ID of traffic being received by the controller as a key field for a flow record:

```
Controller(config)# flow record FLOW-RECORD-1
Controller(config-flow-record)# match datalink vlan input
```

match flow direction

To configure the flow direction as key fields for a flow record, use the **match flow direction** command in flow record configuration or policy inline configuration mode. To disable the use of the flow direction as key fields for a flow record, use the **no** form of this command.

match flow direction

no match flow direction

Syntax Description

This command has no keywords or arguments.

Command Default

The flow direction is not configured as key fields.

Command Modes

Flow record configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

A flow record requires at least one key field before it can be used in a flow monitor. The key fields differentiate flows, with each flow having a unique set of values for the key fields.

The **match flow direction** command indicates the direction of the flow. This feature is most useful when a single flow monitor is configured for input and output flows. It can be used to find and eliminate flows that are being monitored twice, once on input and once on output. This command may also be used to match up pairs of flows in the exported data when the two flows are flowing in opposite directions.

Examples

The following example configures the direction the flow was monitored in as a key field:

```
Controller(config)# flow record FLOW-RECORD-1
Controller(config-flow-record)# match flow direction
```

match interface

To configure the input and output interfaces as key fields for a flow record, use the **match interface** command in flow record configuration mode. To disable the use of the input and output interfaces as key fields for a flow record, use the **no** form of this command.

match interface {**input**| **output**}

no match interface {**input**| **output**}

Syntax Description

input	Configures the input interface as a key field.
output	Configures the output interface as a key field.

Command Default

The input and output interfaces are not configured as key fields.

Command Modes

Flow record configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

A flow record requires at least one key field before it can be used in a flow monitor. The key fields differentiate flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match interface** command.

Examples

The following example configures the input interface as a key field:

```
Controller(config)# flow record FLOW-RECORD-1
Controller(config-flow-record)# match interface input
```

The following example configures the output interface as a key field:

```
Controller(config)# flow record FLOW-RECORD-1
Controller(config-flow-record)# match interface output
```

match ipv4

To configure one or more of the IPv4 fields as a key field for a flow record, use the **match ipv4** command in flow record configuration mode. To disable the use of one or more of the IPv4 fields as a key field for a flow record, use the **no** form of this command.

match ipv4 {**protocol**| **tos**| **version**}

no match ipv4 {**protocol**| **tos**| **version**}

Syntax Description

protocol	Configures the IPv4 protocol as a key field.
tos	Configures the IPv4 ToS as a key field.
version	Configures the IP version from IPv4 header as a key field.

Command Default

The use of one or more of the IPv4 fields as a key field for a user-defined flow record is not enabled by default.

Command Modes

Flow record configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

A flow record requires at least one key field before it can be used in a flow monitor. The key fields differentiate flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

Examples

The following example configures the IPv4 protocol as the key field:

```
Controller(config)# flow record FLOW-RECORD-1
Controller(config-flow-record)# match ipv4 protocol
```

match ipv4 destination address

To configure the IPv4 destination address as a key field for a flow record, use the **match ipv4 destination address** command in flow record configuration mode. To disable the IPv4 destination address as a key field for a flow record, use the **no** form of this command.

match ipv4 destination address

no match ipv4 destination address

Syntax Description

This command has no keywords or arguments.

Command Default

The IPv4 destination address is not configured as a key field.

Command Modes

Flow record configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

A flow record requires at least one key field before it can be used in a flow monitor. The key fields differentiate flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match ipv4 destination address** command.

Examples

The following example configures the IPv4 destination address as a key field for a flow record:

```
Controller(config)# flow record FLOW-RECORD-1
Controller(config-flow-record)# match ipv4 destination address
```

match ipv4 source address

To configure the IPv4 source address as a key field for a flow record, use the **match ipv4 source address** command in flow record configuration mode. To disable the use of the IPv4 source address as a key field for a flow record, use the **no** form of this command.

match ipv4 source address

no match ipv4 source address

Syntax Description

This command has no keywords or arguments.

Command Default

The IPv4 source address is not configured as a key field.

Command Modes

Flow record configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

A flow record requires at least one key field before it can be used in a flow monitor. The key fields differentiate flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match ipv4 source address** command.

Examples

The following example configures the IPv4 source address as a key field:

```
Controller(config)# flow record FLOW-RECORD-1
Controller(config-flow-record)# match ipv4 source address
```

match ipv4 ttl

To configure the IPv4 time-to-live (TTL) field as a key field for a flow record, use the **match ipv4 ttl** command in flow record configuration mode. To disable the use of the IPv4 TTL field as a key field for a flow record, use the **no** form of this command.

match ipv4 ttl

no match ipv4 ttl

Syntax Description

This command has no keywords or arguments.

Command Default

The IPv4 time-to-live (TTL) field is not configured as a key field.

Command Modes

Flow record configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

A flow record requires at least one key field before it can be used in a flow monitor. The key fields differentiate flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match ipv4 ttl** command.

Examples

The following example configures IPv4 TTL as a key field:

```
Controller(config)# flow record FLOW-RECORD-1
Controller(config-flow-record)# match ipv4 ttl
```

match ipv6

To configure one or more of the IPv6 fields as a key field for a flow record, use the **match ipv6** command in flow record configuration mode. To disable the use of one or more of the IPv6 fields as a key field for a flow record, use the **no** form of this command.

match ipv6 {**protocol**| **traffic-class**| **version**}

no match ipv6 {**protocol**| **traffic-class**| **version**}

Syntax Description

protocol	Configures the IPv6 protocol as a key field.
traffic-class	Configures the IPv6 traffic class as a key field.
version	Configures the IPv6 version from IPv6 header as a key field.

Command Default

The IPv6 fields are not configured as a key field.

Command Modes

Flow record configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

A flow record requires at least one key field before it can be used in a flow monitor. The key fields differentiate flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match ipv6** command.

Examples

The following example configures the IPv6 protocol field as a key field:

```
Controller(config)# flow record FLOW-RECORD-1
Controller(config-flow-record)# match ipv6 protocol
```

match ipv6 destination address

To configure the IPv6 destination address as a key field for a flow record, use the **match ipv6 destination address** command in flow record configuration mode. To disable the IPv6 destination address as a key field for a flow record, use the **no** form of this command.

match ipv6 destination address

no match ipv6 destination address

Syntax Description

This command has no keywords or arguments.

Command Default

The IPv6 destination address is not configured as a key field.

Command Modes

Flow record configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

A flow record requires at least one key field before it can be used in a flow monitor. The key fields differentiate flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

Examples

The following example configures the IPv6 destination address as a key field:

```
Controller(config)# flow record FLOW-RECORD-1
Controller(config-flow-record)# match ipv6 destination address
```

match ipv6 hop-limit

To configure the IPv6 hop limit as a key field for a flow record, use the **match ipv6 hop-limit** command in flow record configuration mode. To disable the use of a section of an IPv6 packet as a key field for a flow record, use the **no** form of this command.

match ipv6 hop-limit

no match ipv6 hop-limit

Syntax Description

This command has no keywords or arguments.

Command Default

The use of the IPv6 hop limit as a key field for a user-defined flow record is not enabled by default.

Command Modes

Flow record configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

A flow record requires at least one key field before it can be used in a flow monitor. The key fields differentiate flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

Examples

The following example configures the hop limit of the packets in the flow as a key field:

```
Controller(config)# flow record FLOW-RECORD-1
Controller(config-flow-record)# match ipv6 hop-limit
```

match ipv6 source address

To configure the IPv6 source address as a key field for a flow record, use the **match ipv6 source address** command in flow record configuration mode. To disable the use of the IPv6 source address as a key field for a flow record, use the **no** form of this command.

match ipv6 source address

no match ipv6 source address

Command Default

The IPv6 source address is not configured as a key field.

Command Modes

Flow record configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

A flow record requires at least one key field before it can be used in a flow monitor. The key fields differentiate flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

Examples

The following example configures a IPv6 source address as a key field:

```
Controller(config)# flow record FLOW-RECORD-1
Controller(config-flow-record)# match ipv6 source address
```

match transport

To configure one or more of the transport fields as a key field for a flow record, use the **match transport** command in flow record configuration mode. To disable the use of one or more of the transport fields as a key field for a flow record, use the **no** form of this command.

match transport {**destination-port**| **igmp type**| **source-port**}

no match transport {**destination-port**| **igmp type**| **source-port**}

Syntax Description

destination-port	Configures the transport destination port as a key field.
igmp type	Configures time stamps based on the system uptime as a key field.
source-port	Configures the transport source port as a key field.

Command Default

The transport fields are not configured as a key field.

Command Modes

Flow record configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

A flow record requires at least one key field before it can be used in a flow monitor. The key fields differentiate flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

Examples

The following example configures the destination port as a key field:

```
Controller(config)# flow record FLOW-RECORD-1
Controller(config-flow-record)# match transport destination-port
```

The following example configures the source port as a key field:

```
Controller(config)# flow record FLOW-RECORD-1
Controller(config-flow-record)# match transport source-port
```

match transport icmp ipv4

To configure the ICMP IPv4 type field and the code field as key fields for a flow record, use the **match transport icmp ipv4** command in flow record configuration mode. To disable the use of the ICMP IPv4 type field and code field as key fields for a flow record, use the **no** form of this command.

match transport icmp ipv4 {**code**| **type**}

no match transport icmp ipv4 {**code**| **type**}

Syntax Description

code	Configures the IPv4 ICMP code as a key field.
type	Configures the IPv4 ICMP type as a key field.

Command Default

The ICMP IPv4 type field and the code field are not configured as key fields.

Command Modes

Flow record configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

A flow record requires at least one key field before it can be used in a flow monitor. The key fields differentiate flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

Examples

The following example configures the IPv4 ICMP code field as a key field:

```
Controller(config)# flow record FLOW-RECORD-1
Controller(config-flow-record)# match transport icmp ipv4 code
```

The following example configures the IPv4 ICMP type field as a key field:

```
Controller(config)# flow record FLOW-RECORD-1
Controller(config-flow-record)# match transport icmp ipv4 type
```

match transport icmp ipv6

To configure the ICMP IPv6 type field and the code field as key fields for a flow record, use the **match transport icmp ipv6** command in flow record configuration mode. To disable the use of the ICMP IPv6 type field and code field as key fields for a flow record, use the **no** form of this command.

match transport icmp ipv6 {**code**| **type**}

no match transport icmp ipv6 {**code**| **type**}

Syntax Description

code	Configures the IPv6 ICMP code as a key field.
type	Configures the IPv6 ICMP type as a key field.

Command Default

The ICMP IPv6 type field and the code field are not configured as key fields.

Command Modes

Flow record configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

A flow record requires at least one key field before it can be used in a flow monitor. The key fields differentiate flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

Examples

The following example configures the IPv6 ICMP code field as a key field:

```
Controller(config)# flow record FLOW-RECORD-1
Controller(config-flow-record)# match transport icmp ipv6 code
```

The following example configures the IPv6 ICMP type field as a key field:

```
Controller(config)# flow record FLOW-RECORD-1
Controller(config-flow-record)# match transport icmp ipv6 type
```

option

To configure optional data parameters for a flow exporter for Flexible NetFlow, use the **option** command in flow exporter configuration mode. To remove optional data parameters for a flow exporter, use the **no** form of this command.

option {**exporter-stats**| **interface-table**| **sampler-table**} [**timeout** *seconds*]

no option {**exporter-stats** *seconds*| **interface-table**}

Syntax Description

exporter-stats	Configures the exporter statistics option for flow exporters.
interface-table	Configures the interface table option for flow exporters.
sampler-table	Configures the export sampler table option for flow exporters.
timeout *seconds*	(Optional) Configures the option resend time in seconds for flow exporters. The range is 1 to 86400. The default is 600.

Command Default

The timeout is 600 seconds. All other optional data parameters are not configured.

Command Modes

Flow exporter configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The **option exporter-stats** command causes the periodic sending of the exporter statistics, including the number of records, bytes, and packets sent. This command allows the collector to estimate packet loss for the export records it receives. The optional timeout alters the frequency at which the reports are sent.

The **option interface-table** command causes the periodic sending of an options table, which allows the collector to map the interface SNMP indexes provided in the flow records to interface names. The optional timeout can alter the frequency at which the reports are sent.

Examples

The following example shows how to enable the periodic sending of the exporter statistics, including the number of records, bytes, and packets sent:

```
Controller(config)# flow exporter FLOW-EXPORTER-1
Controller(config-flow-exporter)# option exporter-stats
```

The following example shows how to enable the periodic sending of an options table, which allows the collector to map the interface SNMP indexes provided in the flow records to interface names:

```
Controller(config)# flow exporter FLOW-EXPORTER-1
Controller(config-flow-exporter)# option interface-table
```

template data timeout

To configure the template resend timeout for a flow exporter, use the **template data timeout** command in flow exporter configuration mode. To remove the template resend timeout for a flow exporter, use the **no** form of this command.

template data timeout *seconds*

no template data timeout *seconds*

Syntax Description

seconds	Timeout value in seconds. The range is 1 to 86400. The default is 600.

Command Default

The default template resend timeout for a flow exporter is 600 seconds.

Command Modes

Flow exporter configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

The following example configures resending templates based on a timeout of 1000 seconds:

```
Controller(config)# flow exporter FLOW-EXPORTER-1
Controller(config-flow-exporter)# template data timeout 1000
```

ttl

To configure the time-to-live (TTL) value, use the **ttl** command in flow exporter configuration mode. To remove the TTL value, use the **no** form of this command.

ttl *ttl*

no ttl *ttl*

Syntax Description

ttl	Time-to-live (TTL) value for exported datagrams. The range is 1 to 255. The default is 255.

Command Default

Flow exporters use a TTL of 255.

Command Modes

Flow exporter configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

The following example specifies a TTL of 15:

```
Controller(config)# flow exporter FLOW-EXPORTER-1
Controller(config-flow-exporter)# ttl 15
```

ip flow monitor

To enable a Flexible NetFlow flow monitor for IPv4 traffic that the controller is receiving, use the **ip flow monitor** command in interface configuration mode. To disable a flow monitor, use the **no** form of this command.

ip flow monitor *monitor-name* [**sampler** *sampler-name*] **input**

no ip flow monitor *monitor-name* [**sampler** *sampler-name*] **input**

Syntax Description

monitor-name	Name of the flow monitor to apply to the interface.
sampler *sampler-name*	(Optional) Enables the specified flow sampler for the flow monitor.
input	Monitors IPv4 traffic that the controller receives on the interface.

Command Default

A flow monitor is not enabled.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Before you can apply a flow monitor to an interface with the **ip flow monitor** command, you must have already created the flow monitor using the **flow monitor** global configuration command.

When you add a sampler to a flow monitor, only packets that are selected by the named sampler will be entered into the cache to form flows. Each use of a sampler causes separate statistics to be stored for that usage.

You cannot add a sampler to a flow monitor after the flow monitor has been enabled on the interface. You must first remove the flow monitor from the interface and then enable the same flow monitor with a sampler.

Note The statistics for each flow must be scaled to give the expected true usage. For example, with a 1 in 100 sampler it is expected that the packet and byte counters will have to be multiplied by 100.

Examples

The following example enables a flow monitor for monitoring input traffic:

```
Controller(config)# interface gigabitethernet1/0/1
Controller(config-if)# ip flow monitor FLOW-MONITOR-1 input
```

The following example enables a flow monitor for monitoring input traffic, with a sampler to limit the input packets that are sampled:

```
Controller(config)# interface gigabitethernet1/0/1
Controller(config-if)# ip flow monitor FLOW-MONITOR-1 sampler SAMPLER-1 input
```

The following example shows what happens when you try to add a sampler to a flow monitor that has already been enabled on an interface without a sampler:

```
Controller(config)# interface gigabitethernet1/0/1
Controller(config-if)# ip flow monitor FLOW-MONITOR-1 sampler SAMPLER-2 input
% Flow Monitor: Flow Monitor 'FLOW-MONITOR-1' is already on in full mode and cannot be
enabled with a sampler.
```

The following example shows how to remove a flow monitor from an interface so that it can be enabled with the sampler:

```
Controller(config)# interface gigabitethernet1/0/1
Controller(config-if)# no ip flow monitor FLOW-MONITOR-1 input
Controller(config-if)# ip flow monitor FLOW-MONITOR-1 sampler SAMPLER-2 input
```

ip flow monitor (wireless)

To configure IP NetFlow monitoring, use the **ip flow monitor** command in WLAN configuration mode. To remove IP NetFlow monitoring, use the **no** form of this command.

ip flow monitor *ip-monitor-name* {**input | output**}

no ip flow monitor *ip-monitor-name* {**input | output**}

Syntax Description

ip-monitor-name	Flow monitor name.
input	Enables a flow monitor for ingress traffic.
output	Enables a flow monitor for egress traffic.

Command Default

A flow monitor is not enabled.

Command Modes

WLAN configuration

Usage Guidelines

Before you can apply a flow monitor to an interface with the **datalink flow monitor** command, you must have already created the flow monitor using the **flow monitor** global configuration command.

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to configure an IP flow monitor for ingress traffic:

```
Controller# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# ip flow monitor test input
```

This example shows how to disable an IP flow monitor:

```
Controller# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# no ip flow monitor test input
```

ipv6 flow monitor

To enable a flow monitor for IPv6 traffic that the controller is receiving, use the **ipv6 flow monitor** command in interface configuration mode. To disable a flow monitor, use the **no** form of this command.

ipv6 flow monitor *monitor-name* [**sampler** *sampler-name*] **input**

no ipv6 flow monitor *monitor-name* [**sampler** *sampler-name*] **input**

Syntax Description

monitor-name	Name of the flow monitor to apply to the interface.
sampler *sampler-name*	(Optional) Enables the specified flow sampler for the flow monitor.
input	Monitors IPv6 traffic that the controller receives on the interface.

Command Default

A flow monitor is not enabled.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Before you can apply a flow monitor to the interface with the **ipv6 flow monitor** command, you must have already created the flow monitor using the **flow monitor** global configuration command.

When you add a sampler to a flow monitor, only packets that are selected by the named sampler will be entered into the cache to form flows. Each use of a sampler causes separate statistics to be stored for that usage.

You cannot add a sampler to a flow monitor after the flow monitor has been enabled on the interface. You must first remove the flow monitor from the interface and then enable the same flow monitor with a sampler.

Note The statistics for each flow must be scaled to give the expected true usage. For example, with a 1 in 100 sampler it is expected that the packet and byte counters will have to be multiplied by 100.

Examples

The following example enables a flow monitor for monitoring input traffic:

```
Controller(config)# interface gigabitethernet1/0/1
Controller(config-if)# ipv6 flow monitor FLOW-MONITOR-1 input
```

The following example enables a flow monitor for monitoring input traffic, with a sampler to limit the input packets that are sampled:

```
Controller(config)# interface gigabitethernet1/0/1
Controller(config-if)# ipv6 flow monitor FLOW-MONITOR-1 sampler SAMPLER-1 input
```

The following example shows what happens when you try to add a sampler to a flow monitor that has already been enabled on an interface without a sampler:

```
Controller(config)# interface gigabitethernet1/0/1
Controller(config-if)# ipv6 flow monitor FLOW-MONITOR-1 sampler SAMPLER-2 input
% Flow Monitor: Flow Monitor 'FLOW-MONITOR-1' is already on in full mode and cannot be
enabled with a sampler.
```

The following example shows how to remove a flow monitor from an interface so that it can be enabled with the sampler:

```
Controller(config)# interface gigabitethernet1/0/1
Controller(config-if)# no ipv6 flow monitor FLOW-MONITOR-1 input
Controller(config-if)# ipv6 flow monitor FLOW-MONITOR-1 sampler SAMPLER-2 input
```

ipv6 flow monitor (wireless)

To configure IPv6 NetFlow monitoring, use the **ipv6 flow monitor** command in wlan configuration mode. To remove IPv6 NetFlow monitoring, use the **no** form of this command.

ipv6 flow monitor *ipv6-monitor-name* {**input | output**}

no ipv6 flow monitor *ipv6-monitor-name* {**input | output**}

Syntax Description

ipv6-monitor-name	Flow monitor name.
input	Enables a flow monitor for ingress traffic.
output	Enables a flow monitor for egress traffic.

Command Default

A flow monitor is not enabled.

Command Modes

Wlan configuration

Usage Guidelines

Before you can apply a flow monitor to an interface with the **datalink flow monitor** command, you must have already created the flow monitor using the **flow monitor** global configuration command.

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to configure an IPv6 flow monitor for ingress traffic:

```
Controller# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# ipv6 flow monitor test input
```

This example shows how to disable an IPv6 flow monitor:

```
Controller# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# no ipv6 flow monitor test input
```

show flow exporter

To display flow exporter status and statistics, use the **show flow exporter** command in privileged EXEC mode.

show flow exporter [**export-ids netflow-v9**| [**name**] *exporter-name* [**statistics**| **templates**]| **statistics**| **templates**]

Syntax Description

export-ids netflow-v9	(Optional) Displays the NetFlow Version 9 export fields that can be exported and their IDs.
name	(Optional) Specifies the name of a flow exporter.
exporter-name	(Optional) Name of a flow exporter that was previously configured.
statistics	(Optional) Displays statistics for all flow exporters or for the specified flow exporter.
templates	(Optional) Displays template information for all flow exporters or for the specified flow exporter.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

The following example displays the status and statistics for all of the flow exporters configured on a controller:

```
Controller# show flow exporter
Flow Exporter FLOW-EXPORTER-1:
  Description:              Exports to the datacenter
  Export protocol:          NetFlow Version 9
  Transport Configuration:
    Destination IP address: 172.16.10.2
    Source IP address:      172.16.6.2
    Transport Protocol:     UDP
    Destination Port:       9995
    Source Port:            55864
    DSCP:                   0x0
    TTL:                    255
    Output Features:        Used
```

This table describes the significant fields shown in the display:

Table 21: show flow exporter Field Descriptions

Field	Description
Flow Exporter	The name of the flow exporter that you configured.
Description	The description that you configured for the exporter, or the default description "User defined."
Transport Configuration	The transport configuration fields for this exporter.
Destination IP address	The IP address of the destination host.
Source IP address	The source IP address used by the exported packets.
Transport Protocol	The transport layer protocol used by the exported packets.
Destination Port	The destination UDP port to which the exported packets are sent.
Source Port	The source UDP port from which the exported packets are sent.
DSCP	The differentiated services code point (DSCP) value.
TTL	The time-to-live value.

The following example displays the status and statistics for all of the flow exporters configured on a controller:

```
Controller# show flow exporter name FLOW-EXPORTER-1 statistics
Flow Exporter FLOW-EXPORTER-1:
  Packet send statistics (last cleared 2w6d ago):
    Successfully sent:         0                     (0 bytes)
```

show flow record

To display the status and statistics for a Flexible NetFlow flow record, use the **show flow record** command in privileged EXEC mode.

show flow record [**broker** [**detail**| **picture**]| [**name**] *record-name*]

Syntax Description

broker	(Optional) Displays information about the state of the broker for the Flexible NetFlow flow record.
detail	(Optional) Displays detailed information about the flow record broker.
picture	(Optional) Displays a picture of the broker state.
name	(Optional) Specifies the name of a flow record.
record-name	(Optional) Name of a user-defined flow record that was previously configured.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

The following example displays the status and statistics for FLOW-RECORD-1:

```
Controller# show flow record FLOW-RECORD-1
flow record FLOW-RECORD-1:
  Description:        User defined
  No. of users:       0
  Total field space:  24 bytes
  Fields:
    match ipv4 ttl
    match ipv6 traffic-class
    match ipv6 hop-limit
    match ipv6 destination address
    match transport source-port
    collect interface output
```

show sampler

To display the status and statistics for a Flexible NetFlow sampler, use the **show sampler** command in privileged EXEC mode.

show sampler [**broker** [**detail**| **picture**]| [**name**] *sampler-name*]

Syntax Description

broker	(Optional) Displays information about the state of the broker for the Flexible NetFlow sampler.
detail	(Optional) Displays detailed information about the sampler broker.
picture	(Optional) Displays a picture of the broker state.
name	(Optional) Specifies the name of a sampler.
sampler-name	(Optional) Name of a sampler that was previously configured.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

The following example displays the status and statistics for all of the flow samplers configured:

```
Controller# show sampler
Sampler SAMPLER-1:
  ID:             2083940135
  export ID:      0
  Description:    User defined
  Type:           Invalid (not in use)
  Rate:           1 out of 2
  Samples:        0
  Requests:       0
  Users (0):

Sampler SAMPLER-1:
  ID:             3800923489
  export ID:      1
  Description:    User defined
  Type:           random
  Rate:           1 out of 100
  Samples:        1
  Requests:       124
  Users (1):
```

```
flow monitor FLOW-MONITOR-1 (datalink,vlan1,Output)  0 out of 0
```

This table describes the significant fields shown in the display:

Field	Description
ID	ID number of the flow sampler. This is used to identify the sampler at the collector.
Export ID	ID of the flow sampler export.
Description	Description that you configured for the flow sampler, or the default description "User defined."
Type	Sampling mode that you configured for the flow sampler.
Rate	Window size (for packet selection) that you configured for the flow sampler. The range is 2 to 32768.
Samples	Number of packets sampled since the flow sampler was configured or the controller was restarted. This is equivalent to the number of times a positive response was received when the sampler was queried to determine if the traffic needed to be sampled. See the explanation of the "Requests" field in this table.
Requests	Number of times the flow sampler was queried to determine if the traffic needed to be sampled.
Users	Interfaces on which the flow sampler is configured.

PART XVI

High Availability

High Availability Command Reference

This chapter contains the high availability related commands:

boot system switch

To specify the switches on which the Cisco IOS image is loaded during the next boot cycle, use the **boot system switch** global configuration command. To return to the default setting, use the **no** form of this command.

boot system switch {*stack-member-number* | **all**}

no boot system switch {*stack-member-number* | **all**}

Syntax Description

stack-member-number	The number of the stack member on which to load the Cisco IOS image. The range is 1 to 9. (Specify one stack member only.) This keyword is supported only on stacking-capable switches.
all	Specifies all stack members. This keyword is supported only on stacking-capable switches.

Command Default

The switch attempts to automatically boot up the system by using information in the BOOT environment variable. If this variable is not set, the switch attempts to load and execute the first executable image it can by performing a recursive, depth-first search throughout the flash file system. In a depth-first search of a directory, each encountered subdirectory is completely searched before continuing the search in the original directory.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

On the stack master, use the **boot system switch** *number* command to specify that the software image is loaded on the specified stack member during the next boot cycle. Use the **boot system switch all** command to specify that the software image is loaded on all the stack members during the next boot cycle.

When you enter the **boot system switch** *number* or the **boot system switch all** command on the stack master, the stack master checks if a software image is already on the stack member (except on the stack master). If the software image does not exist on the stack member (for example, stack member 1), an error message such as this appears:

```
%Command to set boot system switch all xxx on switch=1 failed
```

When you enter the **boot system switch** *number* command on the stack master, you can specify only one stack member for the *number* variable. Entering more than one stack member for the *number* variable is not supported.

If you are using the **archive download-sw** privileged EXEC command to maintain system images, you never need to use the **boot system** command. The **boot system** command is automatically manipulated to load the downloaded image.

This command changes the setting of the BOOT environment variable.

mode sso

To set the redundancy mode to stateful switchover (SSO), use the **mode sso** command in redundancy mode.

mode sso

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Redundancy configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The **mode sso** command can be entered only from within redundancy configuration mode.

Follow these guidelines when configuring your system to SSO mode:

- You must use identical Cisco IOS images on the switches in the stack to support SSO mode. Redundancy may not work due to differences between the Cisco IOS releases.
- If you perform an online insertion and removal (OIR) of the module, the switch resets during the stateful switchover and the port states are restarted only if the module is in a transient state (any state other than Ready).
- The forwarding information base (FIB) tables are cleared on a switchover. Routed traffic is interrupted until route tables reconverge.

Examples

This example shows how to set the redundancy mode to SSO:

```
Controller(config)# redundancy
Controller(config-red)# mode sso
Controller(config-red)#
```

redundancy force-switchover

To force a switchover from the active to the standby switch, use the **redundancy force-switchover** command in stateful switchover (SSO) mode on a switch stack.

redundancy force-switchover

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Redundancy SSO

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Use the **redundancy force-switchover** command to manually switch over to the redundant switch. The redundant switch becomes the new active switch that runs the Cisco IOS image, and the modules are reset to their default settings.

The old active switch reboots with the new image and joins the stack.

If you use the **redundancy force-switchover** command on the active switch, the switchports on the active switch to go down.

If you use this command on a switch that is in a partial ring stack, the following warning message appears:

```
Controller# redundancy force-switchover
Stack is in Half ring setup; Reloading a switch might cause stack split
This will reload the active unit and force switchover to standby[confirm]
```

Examples

This example shows how to manually switch over from the active to the standby supervisor engine:

```
Controller# redundancy force-switchover
Controller#
```

set trace capwap ap ha

To trace the control and provisioning of wireless access point high availability, use the **set trace capwap ap ha** command.

set trace capwap ap ha [**detail**| **event**| **dump**] {**filter** [**none** [**switch** *switch*]| *filter_name* [*filter_value* [**switch** *switch*]]]| **level** {**default**| *trace_level*} [**switch** *switch*]}

Syntax Description

detail	(Optional) Specifies the wireless CAPWAP HA details.
event	(Optional) Specifies the wireless CAPWAP HA events.
dump	(Optional) Specifies the wireless CAPWAP HA output.
filter	Specifies the trace Adapted Flag Filter.
none	(Optional) Specifies the no filter option.
switch *switch*	(Optional) Specifies the controller number.
filter_name	Trace adapted flag filter name.
filter_value	(Optional) Value of the filter.
switch *switch*	(Optional) Specifies the controller number.
level	Specifies the trace level.
default	Specifies the unset trace level value.
trace_level	Specifies the trace level.
switch *switch*	(Optional) Specifies the controller number.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples This example shows how to display the wireless CAPWAP HA:

```
Controller# set trace capwap ap ha detail filter mac WORD switch number
```

set trace mobility ha

To debug the wireless mobility high availability in the controller, use the **set trace mobility ha** command.

set trace mobility ha [**event**| **detail**| **dump**] {**filter** [**none** [**switch** *switch*]| *filter_name* [*filter_value* [**switch** *switch*]]]| **level** {**default**| *trace_level*} [**switch** *switch*]}

Syntax Description

event	(Optional) Specifies the wireless mobility HA events.
detail	(Optional) Specifies the wireless mobility HA details.
dump	(Optional) Specifies the wireless mobility HA output.
filter	Specifies to trace adapted flag filter.
none	Specifies no trace adapted flag filter.
switch *switch*	(Optional) Specifies the controller number.
filter_name	Trace adapted flag filter name.
filter_value	Trace adapted flag filter value.
switch *switch*	Specifies the controller number.
level	Specifies the trace level value.
default	Specifies the unset trace level value.
trace_level	Specifies the trace level value.
switch *switch*	Specifies the controller number.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples This example shows how to display wireless mobility HA details:

```
Controller# set trace mobility ha detail filter mac WORD
```

set trace qos ap ha

To trace wireless Quality of Service (QoS) high availability, use the **set trace qos ap ha** command.

set trace QOS ap ha [**event**| **error**] {**filter** [**MACnone** [**switch** *switch*]| *filter_name* [*filter_value* [**switch** *switch*]]]| **level** {**default**| *trace_level*} [**switch** *switch*]}

Syntax Description

event	(Optional) Specifies trace QoS wireless AP event.
event *mac*	Specifies the MAC address of the AP.
event *none*	Specifies no MAC address value.
error	(Optional) Specifies trace QoS wireless AP errors.
error *mac*	Specifies the MAC address of the AP.
error *none*	Specifies no value.
filter	Specifies the trace adapted flag filter.
filter *mac*	Specifies the MAC address of the AP.
filter *none*	Specifies no value.
switch *switch*	Specifies the switch number.
filter_name	(Optional) Specifies the switch filter name.
filter_value	(Optional) Specifies the switch filter value. Value is one.
switch *switch*	(Optional) Specifies the switch number. Value is one.
level	Specifies the trace level.
default	Specifies the trace QoS wireless AP default.
trace_level	Trace level.
switch *switch*	(Optional) Specifies the switch number. Value is one.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to trace wireless QoS high availability:

```
Controller# set trace QOS ap ha
```

show redundancy

To display redundancy facility information, use the **show redundancy** command in privileged EXEC mode

show redundancy [**clients**| **counters**| **history** [**reload**| **reverse**]| **slaves**[*slave-name*] {**clients**| **counters**}| **states**| **switchover history** [**domain default**]]

Syntax Description

clients	(Optional) Displays information about the redundancy facility client.
counters	(Optional) Displays information about the redundancy facility counter.
history	(Optional) Displays a log of past status and related information for the redundancy facility.
history reload	(Optional) Displays a log of past reload information for the redundancy facility.
history reverse	(Optional) Displays a reverse log of past status and related information for the redundancy facility.
slaves	(Optional) Displays all slaves in the redundancy facility.
slave-name	(Optional) The name of the redundancy facility slave to display specific information for. Enter additional keywords to display all clients or counters in the specified slave.
clients	Displays all redundancy facility clients in the specified slave.
counters	Displays all counters in the specified slave.
states	(Optional) Displays information about the redundancy facility state, such as disabled, initialization, standby or active.
switchover history	(Optional) Displays information about the redundancy facility switchover history.
domain default	(Optional) Displays the default domain as the domain to display switchover history for.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to display information about the redundancy facility:

```
Controller# show redundancy
Redundant System Information :
------------------------------
       Available system uptime = 6 days, 9 hours, 23 minutes
Switchovers system experienced = 0
              Standby failures = 0
        Last switchover reason = not known

                 Hardware Mode = Simplex
    Configured Redundancy Mode = SSO
     Operating Redundancy Mode = SSO
              Maintenance Mode = Disabled
                Communications = Down      Reason: Simplex mode

Current Processor Information :
------------------------------
               Active Location = slot 1
        Current Software state = ACTIVE
       Uptime in current state = 6 days, 9 hours, 23 minutes
                 Image Version = Cisco IOS Software, IOS-XE Software, Catalyst 3
850 L3 Switch Software (CAT3850-UNIVERSALK9-M), Version 03.08.59.EMD EARLY DEPLO
YMENT ENGINEERING NOVA_WEEKLY BUILD, synced to DSGS_PI2_POSTPC_FLO_DSBU7_NG3K_11
05
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Sun 16-S
        Configuration register = 0x102

Peer (slot: 0) information is not available because it is in 'DISABLED' state
Controller#
```

This example shows how to display redundancy facility client information:

```
Controller# show redundancy clients
Group ID =     1
     clientID = 20002    clientSeq =     4    EICORE HA Client
     clientID = 24100    clientSeq =     5    WCM_CAPWAP
     clientID = 24101    clientSeq =     6    WCM_RRM HA
     clientID = 24103    clientSeq =     8    WCM_QOS HA
     clientID = 24105    clientSeq =    10    WCM_MOBILITY
     clientID = 24106    clientSeq =    11    WCM_DOT1X
     clientID = 24107    clientSeq =    12    WCM_APFROGUE
     clientID = 24110    clientSeq =    15    WCM_CIDS
     clientID = 24111    clientSeq =    16    WCM_NETFLOW
     clientID = 24112    clientSeq =    17    WCM_MCAST
     clientID = 24120    clientSeq =    18    wcm_comet
     clientID = 24001    clientSeq =    21    Table Manager Client
     clientID = 20010    clientSeq =    24    SNMP SA HA Client
     clientID = 20007    clientSeq =    27    Installer HA Client
     clientID =    29    clientSeq =    60    Redundancy Mode RF
     clientID =   139    clientSeq =    61    IfIndex
     clientID =  3300    clientSeq =    62    Persistent Variable
     clientID =    25    clientSeq =    68    CHKPT RF
     clientID = 20005    clientSeq =    74    IIF-shim
     clientID = 10001    clientSeq =    82    QEMU Platform RF

<output truncated>
```

The output displays the following information:

- clientID displays the client's ID number.
- clientSeq displays the client's notification sequence number.
- Current redundancy facility state.

This example shows how to display the redundancy facility counter information:

```
Controller# show redundancy counters
Redundancy Facility OMs

              comm link up = 0
            comm link down = 0
          invalid client tx = 0
          null tx by client = 0
                tx failures = 0
      tx msg length invalid = 0

      client not rxing msgs = 0
 rx peer msg routing errors = 0
           null peer msg rx = 0
         errored peer msg rx = 0

                 buffers tx = 0
     tx buffers unavailable = 0
                 buffers rx = 0
      buffer release errors = 0

 duplicate client registers = 0
  failed to register client = 0
       Invalid client syncs = 0

Controller#
```

This example shows how to display redundancy facility history information:

```
Controller# show redundancy history
00:00:00 *my state = INITIALIZATION(2) peer state = DISABLED(1)
00:00:00 RF_EVENT_INITIALIZATION(524) op=0 rc=0
00:00:00 *my state = NEGOTIATION(3) peer state = DISABLED(1)
00:00:01 client added: Table Manager Client(24001) seq=21
00:00:01 client added: SNMP SA HA Client(20010) seq=24
00:00:06 client added: WCM_CAPWAP(24100) seq=5
00:00:06 client added: WCM_QOS HA(24103) seq=8
00:00:07 client added: WCM_DOT1X(24106) seq=11
00:00:07 client added: EICORE HA Client(20002) seq=4
00:00:09 client added: WCM_MOBILITY(24105) seq=10
00:00:09 client added: WCM_NETFLOW(24111) seq=16
00:00:09 client added: WCM_APFROGUE(24107) seq=12
00:00:09 client added: WCM_RRM HA(24101) seq=6
00:00:09 client added: WCM_MCAST(24112) seq=17
00:00:09 client added: WCM_CIDS(24110) seq=15
00:00:09 client added: wcm_comet(24120) seq=18
00:00:22 RF_STATUS_REDUNDANCY_MODE_CHANGE(405) First Slave(0) op=0 rc=0
00:00:22 RF_STATUS_REDUNDANCY_MODE_CHANGE(405) Slave(6107) op=0 rc=0
00:00:22 RF_STATUS_REDUNDANCY_MODE_CHANGE(405) Slave(6109) op=0 rc=0
00:00:22 RF_STATUS_REDUNDANCY_MODE_CHANGE(405) Slave(6128) op=0 rc=0
00:00:22 RF_STATUS_REDUNDANCY_MODE_CHANGE(405) Slave(8897) op=0 rc=0
00:00:22 RF_STATUS_REDUNDANCY_MODE_CHANGE(405) Slave(8898) op=0 rc=0
00:00:22 RF_STATUS_REDUNDANCY_MODE_CHANGE(405) Slave(8901) op=0 rc=0
00:00:22 RF_EVENT_SLAVE_STATUS_DONE(523) First Slave(0) op=405 rc=0
00:00:22 RF_STATUS_REDUNDANCY_MODE_CHANGE(405) Redundancy Mode RF(29) op=0 rc=0
00:00:22 RF_STATUS_REDUNDANCY_MODE_CHANGE(405) IfIndex(139) op=0 rc=0

<output truncated>
```

This example shows how to display information about the redundancy facility slaves:

```
Controller# show redundancy slaves
Group ID =   1
Slave/Process ID =  6107   Slave Name = [installer]
```

```
Slave/Process ID =  6109   Slave Name = [eicored]
Slave/Process ID =  6128   Slave Name = [snmp_subagent]
Slave/Process ID =  8897   Slave Name = [wcm]
Slave/Process ID =  8898   Slave Name = [table_mgr]
Slave/Process ID =  8901   Slave Name = [iosd]

Controller#
```

This example shows how to display information about the redundancy facility state:

```
Controller# show redundancy states
         my state = 13 -ACTIVE
       peer state =  1 -DISABLED
             Mode = Simplex
          Unit ID = 1

  Redundancy Mode (Operational) = SSO
   Redundancy Mode (Configured) = SSO
               Redundancy State = Non Redundant
                      Manual Swact = disabled (system is simplex (no peer unit))

   Communications = Down      Reason: Simplex mode

     client count = 75
   client_notification_TMR = 360000 milliseconds
            keep_alive TMR = 9000 milliseconds
          keep_alive count = 0
      keep_alive threshold = 18
             RF debug mask = 0

Controller#
```

show redundancy config-sync

To display a configuration synchronization failure or the ignored mismatched command list (MCL), if any, use the **show redundancy config-sync** command in EXEC mode.

show redundancy config-sync {**failures** {**bem| mcl| prc**}| **ignored failures mcl**}

Syntax Description

failures	Displays MCL entries or best effort method (BEM)/Parser Return Code (PRC) failures.
bem	Displays a BEM failed command list, and forces the standby switch to reboot.
mcl	Displays commands that exist in the switch's running configuration but are not supported by the image on the standby switch, and forces the standby switch to reboot.
prc	Displays a PRC failed command list and forces the standby switch to reboot.
ignored failures mcl	Displays the ignored MCL failures.

Command Default

This command has no default settings.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

When two versions of Cisco IOS images are involved, the command sets supported by two images might differ. If any of those mismatched commands are executed on the active switch, the standby switch might not recognize those commands, which causes a configuration mismatch condition. If the syntax check for the command fails on the standby switch during a bulk synchronization, the command is moved into the MCL and the standby switch is reset. To display all the mismatched commands, use the **show redundancy config-sync failures mcl** command.

To clean the MCL, follow these steps:

1. Remove all mismatched commands from the active switch's running configuration.
2. Revalidate the MCL with a modified running configuration by using the **redundancy config-sync validate mismatched-commands** command.

3 Reload the standby switch.

Alternatively, you could ignore the MCL by following these steps:

1 Enter the **redundancy config-sync ignore mismatched-commands** command.

2 Reload the standby switch; the system transitions to SSO mode.

Note If you ignore the mismatched commands, the out-of-synchronization configuration on the active switch and the standby switch still exists.

3 You can verify the ignored MCL with the **show redundancy config-sync ignored mcl** command.

Each command sets a return code in the action function that implements the command. This return code indicates whether or not the command successfully executes. The active switch maintains the PRC after executing a command. The standby switch executes the command and sends the PRC back to the active switch. A PRC failure occurs if these two PRCs do not match. If a PRC error occurs at the standby switch either during bulk synchronization or line-by-line (LBL) synchronization, the standby switch is reset. To display all PRC failures, use the **show redundancy config-sync failures prc** command.

To display best effort method (BEM) errors, use the **show redundancy config-sync failures bem** command.

Examples

This example shows how to display the BEM failures:

```
Controller> show redundancy config-sync failures bem
BEM Failed Command List
-----------------------

 The list is Empty
```

This example shows how to display the MCL failures:

```
Controller> show redundancy config-sync failures mcl
Mismatched Command List
-----------------------

The list is Empty
```

This example shows how to display the PRC failures:

```
Controller# show redundancy config-sync failures prc
PRC Failed Command List
-----------------------

 The list is Empty
```

show switch

To display information that is related to the stack member or the switch stack, use the **show switch** command in EXEC mode.

Command Default None

Command Modes User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples This example shows how to display summary stack information:

This example shows how to display detailed stack information:

This example shows how to display the member 6 summary information:

```
Controller# show switch 6
Switch#  Role      Mac Address     Priority     State
-----------------------------------------------------
 6       Member     0003.e31a.1e00     1          Ready
```

This example shows how to display the neighbor information for a stack:

```
Controller# show switch neighbors
  Switch #    Port A       Port B
  --------    ------       ------
      6         None          8
      8          6           None
```

This example shows how to display stack-port information:

```
Controller# show switch stack-ports
  Switch #    Port A       Port B
  --------    ------       ------
    6          Down          Ok
    8           Ok          Down
```

This example shows how to display detailed stack-ring activity information for a switch stack:

```
Controller# show switch stack-ring activity detail
Switch   Asic  Rx Queue-1  Rx Queue-2  Rx Queue-3  Rx Queue-4       Total
-------------------------------------------------------------------------
1           0     2021864     1228937      281510           0     3532311
1           1          52           0       72678           0       72730
                                                  ---------------------------
                                                  Switch 1 Total:     3605041
-------------------------------------------------------------------------
2           0     2020901       90833      101680           0     2213414
2           1          52           0           0           0          52
                                                  ---------------------------
                                                  Switch 2 Total:     2213466
-------------------------------------------------------------------------
```

```
Total frames sent to stack ring : 5818507

Note: these counts do not include frames sent to the ring
by certain output features, such as output SPAN and output
ACLs.
```

show trace messages capwap ap ha

To display wireless control and provisioning of wireless access points (CAPWAP) high availability, use the **show trace messages capwap ap ha** command.

show trace messages capwap ap ha [**detail**| **event**| **dump**] [**switch** *switch*]

Syntax Description

detail	(Optional) Displays wireless CAPWAP high availability details.
detail*switch number*	Specifies the controller number. Value is one.
event	(Optional) Displays wireless CAPWAP high availability events.
event*switch number*	Specifies the controller number. Value is one.
dump	(Optional) Displays wireless CAPWAP high availability output.
dump *switch number*	Specifies the controller number. Value is one.
switch	(Optional) Displays the controller number. The value is one.
switch *switch number*	Specifies the controller number. Value is one.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to display CAPWAP high availability output:

```
Controller# show trace messages mobility ha dump switch 1
|  Output modifiers
  <cr>
```

show trace messages mobility ha

To display wireless mobility high availability, use the **show trace messages mobility ha** command.

show trace messages mobility ha [**event**| **detail**| **dump**] [**switch** *switch*]

Syntax Description

event	(Optional) Displays wireless mobility HA events.
event *switch*	Specifies the controller number. Value is one.
detail	(Optional) Displays wireless mobility HA details.
detail *switch*	Specifies the controller number. Value is one.
dump	(Optional) Displays the wireless mobility HA output debugging.
dump *switch*	Specifies the controller number. Value is one.
switch *switch*	(Optional) Displays the controller number.
switch *switch*	Specifies the controller number. Value is one.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to display wireless mobility high availability:

```
Controller# show trace messages mobility ha
```

switch

To disable or enable the specified stack port on the member, use the **switch** command in privileged EXEC mode on a stack member.

switch *stack-member-number* **stack port** *port-number* {**disable| enable**}

Syntax Description

stack-member-number	
stack port *port-number*	Specifies the stack port on the member. The range is 1 to 2.
disable	Disables the specified port.
enable	Enables the specified port.

Command Default

The stack port is enabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

A stack is in the full-ring state when all members are connected through the stack ports and are in the ready state.

The stack is in the partial-ring state when the following occurs:

- All members are connected through their stack ports but some are not in the ready state.
- Some members are not connected through the stack ports.

Note Be careful when using the **switch** *stack-member-number* **stack port** *port-number* **disable** command. When you disable the stack port, the stack operates at half bandwidth.

If you enter the **switch** *stack-member-number* **stack port** *port-number* **disable** privileged EXEC command and the stack is in the full-ring state, you can disable only one stack port. This message appears:

```
Enabling/disabling a stack port may cause undesired stack changes. Continue?[confirm]
```

If you enter the **switch** *stack-member-number* **stack port** *port-number* **disable** privileged EXEC command and the stack is in the partial-ring state, you cannot disable the port. This message appears:

```
Disabling stack port not allowed with current stack configuration.
```

Examples

This example shows how to disable stack port 2 on member 4:

```
Controller# switch 4 stack port 2 disable
```

switch priority

To change the stack member priority value, use the **switch priority** command in global configuration mode on the .

switch *stack-member-number* **priority** *new-priority-value*

Syntax Description

stack-member-number	
new-priority-value	New stack member priority value. The range is 1 to 15.

Command Default

The default priority value is 1.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The new priority value is a factor during an reelection. Therefore when you change the priority value the is not changed immediately.

Examples

This example shows how to change the priority value of stack member 6 to 8:

```
Controller switch 6 priority 8
Changing the Switch Priority of Switch Number 6 to 8
Do you want to continue?[confirm]
```

switch provision

To supply a configuration to a new switch before it joins the switch stack, use the **switch provision** command in global configuration mode on the . To delete all configuration information that is associated with the removed switch (a stack member that has left the stack), use the **no** form of this command.

switch *stack-member-number* **provision** *type*

no switch *stack-member-number* **provision**

Syntax Description

stack-member-number	
type	Switch type of the new switch before it joins the stack. For *type*, enter the model number of a supported switch that is listed in the command-line help strings.

Command Default

The switch is not provisioned.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

To avoid receiving an error message, you must remove the specified switch from the switch stack before using the **no** form of this command to delete a provisioned configuration.

To change the switch type, you must also remove the specified switch from the switch stack. You can change the stack member number of a provisioned switch that is physically present in the switch stack if you do not also change the switch type.

If the switch type of the provisioned switch does not match the switch type in the provisioned configuration on the stack, the switch stack applies the default configuration to the provisioned switch and adds it to the stack. The switch stack displays a message when it applies the default configuration.

Provisioned information appears in the running configuration of the switch stack. When you enter the **copy running-config startup-config** privileged EXEC command, the provisioned configuration is saved in the startup configuration file of the switch stack.

Caution When you use the **switch provision** command, memory is allocated for the provisioned configuration. When a new switch type is configured, the previously allocated memory is not fully released. Therefore, do not use this command more than approximately 200 times, or the switch will run out of memory and unexpected behavior will result.

Examples

This example shows how to provision a switch with a stack member number of 2 for the switch stack. The **show running-config** command output shows the interfaces associated with the provisioned switch.

```
Controller(config)# switch 2 provision WS-xxxx
Controller(config)# end
Controller# show running-config | include switch 2
!
interface GigabitEthernet2/0/1
!
interface GigabitEthernet2/0/2
!
interface GigabitEthernet2/0/3
<output truncated>
```

You also can enter the **show switch** user EXEC command to display the provisioning status of the switch stack.

This example shows how to delete all configuration information about stack member 5 when the switch is removed from the stack:

```
Controller(config)# no switch 5 provision
```

You can verify that the provisioned switch is added to or removed from the running configuration by entering the **show running-config** privileged EXEC command.

switch renumber

To change the stack member number, use the **switch renumber** command in global configuration mode on the .

switch *current-stack-member-number* **renumber** *new-stack-member-number*

Syntax Description

current-stack-member-number	
new-stack-member-number	

Command Default

The default stack member number is 1.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

If another stack member is already using the member number that you just specified, the assigns the lowest available number when you reload the stack member.

Note If you change the number of a stack member, and no configuration is associated with the new stack member number, that stack member loses its current configuration and resets to its default configuration.

Do not use the **switch** *current-stack-member-number* **renumber** *new-stack-member-number* command on a provisioned switch. If you do, the command is rejected.

Use the **reload slot** *current stack member number* privileged EXEC command to reload the stack member and to apply this configuration change.

Examples

This example shows how to change the member number of stack member 6 to 7:

```
Controller(config)# switch 6 renumber 7
WARNING:Changing the switch number may result in a configuration change for that switch.
The interface configuration associated with the old switch number will remain as a provisioned
 configuration.
Do you want to continue?[confirm]
```

PART XVII

Network Management

Network Management Commands

This chapter contains all product dependent Network Management commands.

debug spanning-tree

To enable debugging of spanning-tree activities, use the **debug spanning-tree** command in EXEC mode. To disable debugging, use the **no** form of this command.

debug spanning-tree {**all | backbonefast | bpdu | bpdu-opt | config** | **csuf/csrt | etherchannel | events | exceptions | general | mstp | pvst+| root | snmp | synchronization | switch | uplinkfast**}

no debug spanning-tree {**all | backbonefast | bpdu | bpdu-opt | config** | **csuf/csrt | etherchannel | events | exceptions | general | mstp | pvst+| root | snmp | synchronization | switch | uplinkfast**}

Syntax Description

all	Displays all spanning-tree debug messages.
backbonefast	Displays BackboneFast-event debug messages.
bpdu	Displays spanning-tree bridge protocol data unit (BPDU) debug messages.
bpdu-opt	Displays optimized BPDU handling debug messages.
config	Displays spanning-tree configuration change debug messages.
csuf/csrt	Displays cross-stack UplinkFast and cross-stack rapid transition activity debug messages. This keyword is supported only on stacking-capable controllers.
etherchannel	Displays EtherChannel-support debug messages.
events	Displays spanning-tree topology event debug messages.
exceptions	Displays spanning-tree exception debug messages.
general	Displays general spanning-tree activity debug messages.
mstp	Debugs Multiple Spanning Tree Protocol (MSTP) events.
pvst+	Displays per-VLAN spanning-tree plus (PVST+) event debug messages.
root	Displays spanning-tree root-event debug messages.
snmp	Displays spanning-tree Simple Network Management Protocol (SNMP) handling debug messages.
synchronization	Displays the spanning-tree synchronization event debug messages.
switch	Displays controller shim command debug messages. This shim is the software module that is the interface between the generic Spanning Tree Protocol (STP) code and the platform-specific code of various controller platforms.
uplinkfast	Displays UplinkFast-event debug messages.

Command Default Debugging is disabled.

Command Modes Privileged EXEC

Command History

Release	Modification
	This command was introduced.

Usage Guidelines The **undebug spanning-tree** command is the same as the **no debug spanning-tree** command.

When you enable debugging on a switch stack, it is enabled only on the . To enable debugging on a stack member, start a session from the by using the **session***switch-number* command in privileged EXEC mode. Then enter the **debug** command at the command-line prompt of the stack member. To enable debugging on a stack member without first starting a session on the , use the **remote command** *switch-number LINE* command in privileged EXEC mode.

show ip sla statistics

To display current or aggregated operational status and statistics of all Cisco IOS IP Service Level Agreement (SLA) operations or a specified operation, use the **show ip sla statistics** command in user EXEC or privileged EXEC mode.

show ip sla statistics [*operation-number* [**details**] | **aggregated** [*operation-number* | **details**] | **details**]

Syntax Description

operation-number	(Optional) Number of the operation for which operational status and statistics are displayed. Accepted values are from 1 to 2147483647.
details	(Optional) Specifies detailed output.
aggregated	(Optional) Specifies the IP SLA aggregated statistics.

Command Default

Displays output for all running IP SLA operations.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Use the **show ip sla statistics** to display the current state of IP SLA operations, including how much life the operation has left, whether the operation is active, and the completion time. The output also includes the monitoring data returned for the last (most recently completed) operation. This generated operation ID is displayed when you use the **show ip sla** configuration command for the base multicast operation, and as part of the summary statistics for the entire operation.

Enter the **show** command for a specific operation ID to display details for that one responder.

Examples

The following is sample output from the **show ip sla statistics** command:

```
Controller# show ip sla statistics

Current Operational State
Entry Number: 3
Modification Time: *22:15:43.000 UTC Sun Feb 11 2001
Diagnostics Text:
Last Time this Entry was Reset: Never
Number of Octets in use by this Entry: 1332
Number of Operations Attempted: 2
Current Seconds Left in Life: 3511
Operational State of Entry: active
```

```
Latest Completion Time (milliseconds): 544
Latest Operation Start Time: *22:16:43.000 UTC Sun Feb 11 2001
Latest Oper Sense: ok
Latest Sense Description: 200  OK
Total RTT: 544
DNS RTT: 12
TCP Connection RTT: 28
HTTP Transaction RTT: 504
HTTP Message Size: 9707
```

show monitor

To display information about all Switched Port Analyzer (SPAN) and Remote SPAN (RSPAN) sessions, use the **show monitor** command in EXEC mode.

show monitor [**session** {*session_number* | **all** | **local** | **range** *list* | **remote**} [**detail**]]

Syntax Description

session	(Optional) Displays information about specified SPAN sessions.
session_number	
all	(Optional) Displays all SPAN sessions.
local	(Optional) Displays only local SPAN sessions.
range *list*	(Optional) Displays a range of SPAN sessions, where *list* is the range of valid sessions. The range is either a single session or a range of sessions described by two numbers, the lower one first, separated by a hyphen. Do not enter any spaces between comma-separated parameters or in hyphen-specified ranges. **Note** This keyword is available only in privileged EXEC mode.
remote	(Optional) Displays only remote SPAN sessions.
detail	(Optional) Displays detailed information about the specified sessions.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The output is the same for the **show monitor** command and the **show monitor session all** command.

Examples

This is an example of output for the **show monitor** user EXEC command:

```
Controller# show monitor
```

```
Session 1
---------
Type : Local Session
Source Ports :
RX Only : Gi4/0/1
Both : Gi4/0/2-3,Gi4/0/5-6
Destination Ports : Gi4/0/20
Encapsulation : Replicate
Ingress : Disabled
Session 2
---------
Type : Remote Source Session
Source VLANs :
TX Only : 10
Both : 1-9
Dest RSPAN VLAN : 105
```

This is an example of output for the **show monitor** user EXEC command for local SPAN source session 1:

```
Controller# show monitor session 1
Session 1
---------
Type : Local Session
Source Ports :
RX Only : Gi4/0/1
Both : Gi4/0/2-3,Gi4/0/5-6
Destination Ports : Gi4/0/20
Encapsulation : Replicate
Ingress : Disabled
```

This is an example of output for the **show monitor session all** user EXEC command when ingress traffic forwarding is enabled:

```
Controller# show monitor session all
Session 1
---------
Type : Local Session
Source Ports :
Both : Gi4/0/2
Destination Ports : Gi4/0/3
Encapsulation : Native
Ingress : Enabled, default VLAN = 5
Ingress encap : DOT1Q
Session 2
---------
Type : Local Session
Source Ports :
Both : Gi4/0/8
Destination Ports : Gi4/012
Encapsulation : Replicate
Ingress : Enabled, default VLAN = 4
Ingress encap : Untagged
```

show platform ip wccp

To display platform-dependent Web Cache Communication Protocol (WCCP) information, use the **show platform ip wccp** privileged EXEC command.

show platform ip wccp {**cache-engines | interfaces | service-groups**} [**switch** *switch-number*]

Syntax Description

cache-engines	Displays WCCP cache engines.
interfaces	Displays WCCP interfaces.
service-groups	Displays WCCP service groups.
switch *switch-number*	(Optional) Displays WCCP information only for specified *switch-number*.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Use this command only when you are working directly with a technical support representative while troubleshooting a problem. Do not use this command unless a technical support representative asks you to do so.

This command is available only if your controller is running the IP Services feature set.

Examples

The following example displays WCCP interfaces:

```
Controller# show platform ip wccp interfaces

WCCP Interfaces


**** WCCP Interface Gi1/0/3 iif_id:0x104a60000000087 (#SG:1), vrf:0 Ingress
le_handle:0x565dd208 IPv4 Sw-Label:3, Asic-Label:3

* Service group id:0 type: Well-known    token:126 vrf:0 (ref count:1)
Open service    prot: PROT_TCP  l4_type: Dest ports     priority: 240
port[0]: 80
```

snmp-server enable traps

To enable the controller to send Simple Network Management Protocol (SNMP) notifications for various traps or inform requests to the network management system (NMS), use the **snmp-server enable traps** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps [**auth-framework** | **bridge** | **bulkstat** | **call-home** | **cef** | **config** | **config-copy** | **config-ctid** | **copy-config** | **cpu** | **cpu threshold** | **entity** | **envmon** | **errdisable** | **event-manager** | **flash** | **flowmon** | **fru-ctrl** | **ipmulticast** | **ipsla** | **license** | **local-auth** | **mac-notification** | **memory** | **msdp** | **pim** | **power-ethernet** | **rf** | **snmp** | **stackwise** | **storm-control** | **stpx** | **syslog** | **transceiver** | **tty** | **vlan-membership** | **vlancreate** | **vlandelete** | **vrfmib** | **vtp** | **wireless**]

no snmp-server enable traps [**auth-framework** | **bridge** | **bulkstat** | **call-home** | **cef** | **config** | **config-copy** | **config-ctid** | **copy-config** | **cpu** | **cpu threshold** | **entity** | **envmon** | **errdisable** | **event-manager** | **flash** | **flowmon** | **fru-ctrl** | **ipmulticast** | **ipsla** | **license** | **local-auth** | **mac-notification** | **memory** | **msdp** | **pim** | **power-ethernet** | **rf** | **snmp** | **stackwise** | **storm-control** | **stpx** | **syslog** | **transceiver** | **tty** | **vlan-membership** | **vlancreate** | **vlandelete** | **vrfmib** | **vtp** | **wireless**]

Syntax Description

auth-framework	(Optional) Enables SNMP CISCO-AUTH-FRAMEWORK-MIB traps.
bridge	(Optional) Enables SNMP STP Bridge MIB traps.*
bulkstat	(Optional) Enables Data-Collection-MIB Collection notification traps.*
call-home	(Optional) Enables SNMP CISCO-CALLHOME-MIB traps.*
cef	(Optional) Enables cluster traps.*
config	(Optional) Enables SNMP configuration traps.
config-copy	(Optional) Enables SNMP configuration copy traps.
config-ctid	(Optional) Enables SNMP configuration CTID traps.
copy-config	(Optional) Enables SNMP copy-configuration traps.
cpu	(Optional) Enables CPU notification traps.*
cpu threshold	(Optional) Enables CPU threshold notification traps.
entity	(Optional) Enables SNMP entity traps.
envmon	(Optional) Enables SNMP environmental monitor traps.*
errdisable	(Optional) Enables SNMP errdisable notification traps.*
event-manager	(Optional) Enables SNMP Embedded Event Manager traps.

flash	(Optional) Enables SNMP FLASH notification traps.*
flowmon	(Optional) Enables SNMP flowmon notification traps.
fru-ctrl	(Optional) Generates entity field-replaceable unit (FRU) control traps. In a controller stack, this trap refers to the insertion or removal of a controller in the stack.
ipmulticast	(Optional) Enables IP multicast routing traps.
ipsla	(Optional) Enables SNMP IP SLA traps.
license	(Optional) Enables license traps.*
local-auth	(Optional) Enables SNMP local auth traps.
mac-notification	(Optional) Enables SNMP MAC Notification traps.*
memory	(Optional) Enables MEMORY traps.
msdp	(Optional) Enables Multicast Source Discovery Protocol (MSDP) traps.
pim	(Optional) Enables SNMP PIM traps.*
power-ethernet	(Optional) Enables SNMP power Ethernet traps.*
rf	(Optional) Enables all SNMP traps defined in CISCO-RF-MIB.
snmp	(Optional) Enables SNMP traps.*
stackwise	(Optional) Enables SNMP stackwise traps.*
storm-control	(Optional) Enables SNMP storm-control trap parameters.*
stpx	(Optional) Enables SNMP STPX MIB traps.*
syslog	(Optional) Enables SNMP syslog traps.
transceiver	(Optional) Enables SNMP transceiver traps.*
tty	(Optional) Sends TCP connection traps. This is enabled by default.
vlan-membership	(Optional) Enables SNMP VLAN membership traps.
vlancreate	(Optional) Enables SNMP VLAN-created traps.
vlandelete	(Optional) Enables SNMP VLAN-deleted traps.
vrfmib	(Optional) Enables SNMP vrfmib traps.*
vtp	(Optional) Enables VLAN Trunking Protocol (VTP) traps.

wireless	(Optional) Enables wireless traps.

Command Default

The sending of SNMP traps is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The command options marked with an asterisk in the table above have subcommands. For more information on these subcommands, see the Related Commands section below.

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

When supported, use the **snmp-server enable traps** command to enable sending of traps or informs.

Note Though visible in the command-line help strings, the **fru-ctrl, insertion**, and **removal** keywords are not supported on the controller. The **snmp-server enable informs** global configuration command is not supported. To enable the sending of SNMP inform notifications, use the **snmp-server enable traps** global configuration command combined with the **snmp-server host** *host-addr* **informs** global configuration command.

Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

Examples

This example shows how to enable more than one type of SNMP trap:

```
Controller(config)# snmp-server enable traps cluster
Controller(config)# snmp-server enable traps config
Controller(config)# snmp-server enable traps vtp
```

Related Commands

Command	Description
snmp-server enable traps bridge	Generates STP bridge MIB traps.
snmp-server enable traps bulkstat	Enables data-collection-MIB notifications.

Command	Description
snmp-server enable traps call-home	Enables SNMP CISCO-CALLHOME-MIB traps.
snmp-server enable traps cef	Enables SNMP CEF traps.
snmp-server enable traps cpu	Enables CPU notifications.
snmp-server enable traps envmon	Enables SNMP environmental traps.
snmp-server enable traps errdisable	Enables SNMP errdisable notifications.
snmp-server enable traps flash	Enables SNMP flash notifications.
snmp-server enable traps license	Enables license traps.
snmp-server enable traps mac-notification	Enables SNMP MAC notification traps.
snmp-server enable traps pim	Enables SNMP PIM traps.
snmp-server enable traps power-ethernet	Enables SNMP PoE traps.
snmp-server enable traps snmp	Enables SNMP traps.
snmp-server enable traps stackwise	Enables SNMP stackwise traps.
snmp-server enable traps storm-control	Enables SNMP storm-control trap parameters.
snmp-server enable traps stpx	Enables SNMP STPX MIB traps.
snmp-server enable traps transceiver	Enable SNMP transceiver traps.
snmp-server enable traps vrfmib	Allows SNMP vrfmib traps.
snmp-server enable traps wireless	Command to configure trap for wireless parameters.
snmp-server host	Specifies the recipient (host) of a SNMP notification operation.

snmp-server enable traps bridge

To generate STP bridge MIB traps, use the **snmp-server enable traps bridge** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps bridge [**newroot**] [**topologychange**]

no snmp-server enable traps bridge [**newroot**] [**topologychange**]

Syntax Description

newroot	(Optional) Enables SNMP STP bridge MIB new root traps.
topologychange	(Optional) Enables SNMP STP bridge MIB topology change traps.

Command Default

The sending of bridge SNMP traps is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

Examples

This example shows how to send bridge new root traps to the NMS:

```
Controller(config)# snmp-server enable traps bridge newroot
```

snmp-server enable traps bulkstat

To enable data-collection-MIB traps, use the **snmp-server enable traps bulkstat** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps bulkstat [**collection** | **transfer**]

no snmp-server enable traps bulkstat [**collection** | **transfer**]

Syntax Description

collection	(Optional) Enables data-collection-MIB collection traps.
transfer	(Optional) Enables data-collection-MIB transfer traps.

Command Default

The sending of data-collection-MIB traps is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

Examples

This example shows how to generate data-collection-MIB collection traps:

```
Controller(config)# snmp-server enable traps bulkstat collection
```

snmp-server enable traps call-home

To enable SNMP CISCO-CALLHOME-MIB traps, use the **snmp-server enable traps call-home** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps call-home [**message-send-fail** | **server-fail**]

no snmp-server enable traps call-home [**message-send-fail** | **server-fail**]

Syntax Description

message-send-fail	(Optional) Enables SNMP message-send-fail traps.
server-fail	(Optional) Enable SNMP server-fail traps.

Command Default

The sending of SNMP CISCO-CALLHOME-MIB traps is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

Examples

This example shows how to generate SNMP message-send-fail traps:

```
Controller(config)# snmp-server enable traps call-home message-send-fail
```

snmp-server enable traps cef

To enable SNMP Cisco Express Forwarding (CEF) traps, use the **snmp-server enable traps cef** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps cef [**inconsistency** | **peer-fib-state-change** | **peer-state-change** | **resource-failure**]

no snmp-server enable traps cef [**inconsistency** | **peer-fib-state-change** | **peer-state-change** | **resource-failure**]

Syntax Description

inconsistency	(Optional) Enables SNMP CEF Inconsistency traps.
peer-fib-state-change	(Optional) Enables SNMP CEF Peer FIB State change traps.
peer-state-change	(Optional) Enables SNMP CEF Peer state change traps.
resource-failure	(Optional) Enables SNMP CEF Resource Failure traps.

Command Default

The sending of SNMP CEF traps is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

Examples

This example shows how to generate SNMP CEF inconsistency traps:

```
Controller(config)# snmp-server enable traps cef inconsistency
```

snmp-server enable traps cpu

To enable CPU notifications, use the **snmp-server enable traps cpu** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps cpu [**threshold**]

no snmp-server enable traps cpu [**threshold**]

Syntax Description

threshold	(Optional) Enables CPU threshold notification.

Command Default

The sending of CPU notifications is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

Examples

This example shows how to generate CPU threshold notifications:

```
Controller(config)# snmp-server enable traps cpu threshold
```

snmp-server enable traps envmon

To enable SNMP environmental traps, use the **snmp-server enable traps envmon** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps envmon [**fan** | **shutdown** | **status** | **supply** | **temperature**]

no snmp-server enable traps envmon [**fan** | **shutdown** | **status** | **supply** | **temperature**]

Syntax Description

fan	(Optional) Enables fan traps.
shutdown	(Optional) Enables environmental monitor shutdown traps.
status	(Optional) Enables SNMP environmental status-change traps.
supply	(Optional) Enables environmental monitor power-supply traps.
temperature	(Optional) Enables environmental monitor temperature traps.

Command Default

The sending of environmental SNMP traps is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

Examples

This example shows how to generate fan traps:

```
Controller(config)# snmp-server enable traps envmon fan
```

snmp-server enable traps errdisable

To enable SNMP notifications of error-disabling, use the **snmp-server enable traps errdisable** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps errdisable [**notification-rate** *number-of-notifications*]

no snmp-server enable traps errdisable [**notification-rate** *number-of-notifications*]

Syntax Description

notification-rate *number-of-notifications*	(Optional) Specifies number of notifications per minute as the notification rate. Accepted values are from 0 to 4294967295.

Command Default

The sending of SNMP notifications of error-disabling is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

Examples

This example shows how to set the number SNMP notifications of error-disabling to 2:

```
Controller(config)# snmp-server enable traps errdisable notification-rate 2
```

snmp-server enable traps flash

To enable SNMP flash notifications, use the **snmp-server enable traps flash** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps flash [**insertion** | **removal**]

no snmp-server enable traps flash [**insertion** | **removal**]

Syntax Description

insertion	(Optional) Enables SNMP flash insertion notifications.
removal	(Optional) Enables SNMP flash removal notifications.

Command Default

The sending of SNMP flash notifications is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

Examples

This example shows how to generate SNMP flash insertion notifications:

```
Controller(config)# snmp-server enable traps flash insertion
```

snmp-server enable traps license

To enable license traps, use the **snmp-server enable traps license** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps license [**deploy** | **error** | **usage**]

no snmp-server enable traps license [**deploy** | **error** | **usage**]

Syntax Description

deploy	(Optional) Enables license deployment traps.
error	(Optional) Enables license error traps.
usage	(Optional) Enables license usage traps.

Command Default

The sending of license traps is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

Examples

This example shows how to generate license deployment traps:

```
Controller(config)# snmp-server enable traps license deploy
```

snmp-server enable traps mac-notification

To enable SNMP MAC notification traps, use the **snmp-server enable traps mac-notification** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps mac-notification [**change** | **move** | **threshold**]

no snmp-server enable traps mac-notification [**change** | **move** | **threshold**]

Syntax Description

change	(Optional) Enables SNMP MAC change traps.
move	(Optional) Enables SNMP MAC move traps.
threshold	(Optional) Enables SNMP MAC threshold traps.

Command Default

The sending of SNMP MAC notification traps is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

Examples

This example shows how to generate SNMP MAC notification change traps:

```
Controller(config)# snmp-server enable traps mac-notification change
```

snmp-server enable traps pim

To enable SNMP Protocol-Independent Multicast (PIM) traps, use the **snmp-server enable traps pim** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps pim [**invalid-pim-message** | **neighbor-change** | **rp-mapping-change**]

no snmp-server enable traps pim [**invalid-pim-message** | **neighbor-change** | **rp-mapping-change**]

Syntax Description

invalid-pim-message	(Optional) Enables invalid PIM message traps.
neighbor-change	(Optional) Enables PIM neighbor-change traps.
rp-mapping-change	(Optional) Enables rendezvous point (RP)-mapping change traps.

Command Default

The sending of PIM SNMP traps is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

Examples

This example shows how to enable invalid PIM message traps:

```
Controller(config)# snmp-server enable traps pim invalid-pim-message
```

snmp-server enable traps power-ethernet

To enable SNMP power-over-Ethernet (PoE) traps, use the **snmp-server enable traps power-ethernet** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps power-ethernet {**group** *name* | **police**}

no snmp-server enable traps power-ethernet {**group** *name* | **police**}

Syntax Description

group *name*	Enables inline power group-based traps for the specified group number or list.
police	Enables inline power policing traps.

Command Default

The sending of power-over-Ethernet SNMP traps is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

Examples

This example shows how to enable power-over-Ethernet traps for group poe1:

```
Controller(config)# snmp-server enable traps poower-over-ethernet group poe1
```

snmp-server enable traps snmp

To enable SNMP traps, use the **snmp-server enable traps snmp** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps snmp [**authentication | coldstart | linkdown | linkup | warmstart**]

no snmp-server enable traps snmp [**authentication | coldstart | linkdown | linkup | warmstart**]

Syntax Description

authentication	(Optional) Enables authentication traps.
coldstart	(Optional) Enables cold start traps.
linkdown	(Optional) Enables linkdown traps.
linkup	(Optional) Enables linkup traps.
warmstart	(Optional) Enables warmstart traps.

Command Default

The sending of SNMP traps is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

Examples

This example shows how to enable a warmstart SNMP trap:

```
Controller(config)# snmp-server enable traps snmp warmstart
```

snmp-server enable traps stackwise

To enable SNMP stackwise traps, use the **snmp-server enable traps stackwise** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps stackwise [**GLS** | **ILS** | **SRLS** | **insufficient-power** | **invalid-input-current** | **invalid-output-current** | **member-removed** | **member-upgrade-notification** | **new-master** | **new-memberport-change** | **power-budget-warning** | **power-invalid-topology** | **power-link-status-changed** | **power-oper-status-changed** | **power-priority-conflict** | **power-version-mismatch** | **ring-redundant** | **stack-mismatch** | **unbalanced-power-supplies** | **under-budget** | **under-voltage**]

no snmp-server enable traps stackwise [**GLS** | **ILS** | **SRLS** | **insufficient-power** | **invalid-input-current** | **invalid-output-current** | **member-removed** | **member-upgrade-notification** | **new-master** | **new-memberport-change** | **power-budget-warning** | **power-invalid-topology** | **power-link-status-changed** | **power-oper-status-changed** | **power-priority-conflict** | **power-version-mismatch** | **ring-redundant** | **stack-mismatch** | **unbalanced-power-supplies** | **under-budget** | **under-voltage**]

Syntax Description

GLS	(Optional) Enables stackwise stack power GLS trap.
ILS	(Optional) Enables stackwise stack power ILS trap.
SRLS	(Optional) Enables stackwise stack power SRLS trap.
insufficient-power	(Optional) Enables stackwise stack power unbalanced power supplies trap.
invalid-input-current	(Optional) Enables stackwise stack power invalid input current trap.
invalid-output-current	(Optional) Enables stackwise stack power invalid output current trap.
member-removed	(Optional) Enables stackwise stack member removed trap.
member-upgrade-notification	(Optional) Enables stackwise member to be reloaded for upgrade trap.
new-master	(Optional) Enables stackwise new master trap.

Syntax Description

new-memberport-change	(Optional) Enables stackwise stack new memberport trap.
power-budget-warning	(Optional) Enables stackwise stack power budget warning trap.
power-invalid-topology	(Optional) Enables stackwise stack power invalid topology trap.
power-link-status-changed	(Optional) Enables stackwise stack power link status changed trap.
power-oper-status-changed	(Optional) Enables stackwise stack power port oper status changed trap.

power-priority-conflict	(Optional) Enables stackwise stack power priority conflict trap.
power-version-mismatch	(Optional) Enables stackwise stack power version mismatch discovered trap.
ring-redundant	(Optional) Enables stackwise stack ring redundant trap.
stack-mismatch	(Optional) Enables stackwise stack mismatch trap.
unbalanced-power-supplies	(Optional) Enables stackwise stack power unbalanced power supplies trap.
under-budget	(Optional) Enables stackwise stack power under budget trap.
under-voltage	(Optional) Enables stackwise stack power under voltage trap.

Command Default The sending of SNMP stackwise traps is disabled.

Command Modes Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

Examples This example shows how to generate stackwise stack power GLS traps:

```
Controller(config)# snmp-server enable traps stackwise GLS
```

snmp-server enable traps storm-control

To enable SNMP storm-control trap parameters, use the **snmp-server enable traps storm-control** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps storm-control {**trap-rate** *number-of-minutes*}

no snmp-server enable traps storm-control {**trap-rate** *number-of-minutes*}

Syntax Description

trap-rate *number-of-minutes*	(Optional) Specifies the SNMP storm-control trap rate in minutes. Accepted values are from 0 to 1000.

Command Default

The sending of SNMP storm-control trap parameters is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

Examples

This example shows how to set the SNMP storm-control trap rate to 10 traps per minute:

```
Controller(config)# snmp-server enable traps storm-control trap-rate 10
```

snmp-server enable traps stpx

To enable SNMP STPX MIB traps, use the **snmp-server enable traps stpx** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps stpx [**inconsistency** | **loop-inconsistency** | **root-inconsistency**]

no snmp-server enable traps stpx [**inconsistency** | **loop-inconsistency** | **root-inconsistency**]

Syntax Description

inconsistency	(Optional) Enables SNMP STPX MIB inconsistency update traps.
loop-inconsistency	(Optional) Enables SNMP STPX MIB loop inconsistency update traps.
root-inconsistency	(Optional) Enables SNMP STPX MIB root inconsistency update traps.

Command Default

The sending of SNMP STPX MIB traps is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

Examples

This example shows how to generate SNMP STPX MIB inconsistency update traps:

```
Controller(config)# snmp-server enable traps stpx inconsistency
```

snmp-server enable traps transceiver

To enable SNMP transceiver traps, use the **snmp-server enable traps transceiver** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps transceiver [**all**]

no snmp-server enable traps transceiver [**all**]

Syntax Description

all	(Optional) Enables all SNMP transceiver traps.

Command Default

The sending of SNMP transceiver traps is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

Examples

This example shows how to set all SNMP transceiver traps:

```
Controller(config)# snmp-server enable traps transceiver all
```

snmp-server enable traps vrfmib

To allow SNMP vrfmib traps, use the **snmp-server enable traps vrfmib** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps vrfmib [**vnet-trunk-down** | **vnet-trunk-up** | **vrf-down** | **vrf-up**]

no snmp-server enable traps vrfmib [**vnet-trunk-down** | **vnet-trunk-up** | **vrf-down** | **vrf-up**]

Syntax Description

vnet-trunk-down	(Optional) Enables vrfmib trunk down traps.
vnet-trunk-up	(Optional) Enables vrfmib trunk up traps.
vrf-down	(Optional) Enables vrfmib vrf down traps.
vrf-up	(Optional) Enables vrfmib vrf up traps.

Command Default

The sending of SNMP vrfmib traps is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

Examples

This example shows how to generate vrfmib trunk down traps:

```
Controller(config)# snmp-server enable traps vrfmib vnet-trunk-down
```

snmp-server enable traps wireless

To enable sending Simple Network Management Protocol (SNMP) notifications for various wireless traps or inform requests to the network management system (NMS), use the **snmp-server enable traps wireless** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps wireless [**AP | RRM | bsn80211SecurityTrap | bsnAPParamUpdate | bsnAPProfile | bsnAccessPoint | bsnMobileStation | bsnRogue | client | mfp | rogue**]

no snmp-server enable traps wireless [**AP | RRM | bsn80211SecurityTrap | bsnAPParamUpdate | bsnAPProfile | bsnAccessPoint | bsnMobileStation | bsnRogue | client | mfp | rogue**]

Syntax Description

AP	(Optional) Enables sending of AP related traps.
RRM	(Optional) Enables sending of RRM traps.
bsn80211SecurityTrap	(Optional) Enables security-related traps.
bsnAPParamUpdate	(Optional) Enables sending of traps for AP parameters that get updated.
bsnAPProfile	(Optional) Enables BSN AP profile traps.
bsnAccessPoint	(Optional) Enables access point traps.
bsnMobileStation	(Optional) Controls wireless client traps.
bsnRogue	(Optional) Enables rogue-related traps.
client	(Optional) Enables client traps.
mfp	(Optional) Enables MFP traps.
rogue	(Optional) Enables rogue traps.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

Examples

This example shows how to generate sending AP related wireless traps:

```
Controller(config)# snmp-server enable traps wireless ap
```

snmp-server engineID

To configure a name for either the local or remote copy of SNMP, use the **snmp-server engineID** command in global configuration mode.

snmp-server engineID {**local** *engineid-string* | **remote** *ip-address* [**udp-port** *port-number*] *engineid-string*}

Syntax Description

local *engineid-string*	Specifies a 24-character ID string with the name of the copy of SNMP. You need not specify the entire 24-character engine ID if it has trailing zeros. Specify only the portion of the engine ID up to the point where only zeros remain in the value.
remote *ip-address*	Specifies the remote SNMP copy. Specify the *ip-address* of the device that contains the remote copy of SNMP.
udp-port *port-number*	(Optional) Specifies the User Datagram Protocol (UDP) port on the remote device. The default is 162.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

None

Examples

The following example configures a local engine ID of 123400000000000000000000:

```
Controller(config)# snmp-server engineID local 1234
```

snmp-server host

To specify the recipient (host) of a Simple Network Management Protocol (SNMP) notification operation, use the **snmp-server host** global configuration command on the controller. Use the **no** form of this command to remove the specified host.

snmp-server host {*host-addr* } [**vrf** *vrf-instance*] [**informs** | **traps**] [**version** {**1** | **2c** | **3** {**auth** | **noauth** | **priv**} }] {*community-string* [*notification-type*] }

no snmp-server host {*host-addr* } [**vrf** *vrf-instance*] [**informs** | **traps**] [**version** {**1** | **2c** | **3** {**auth** | **noauth** | **priv**} }] {*community-string* [*notification-type*] }

Syntax Description

host-addr	Name or Internet address of the host (the targeted recipient).
vrf *vrf-instance*	(Optional) Specifies the virtual private network (VPN) routing instance and name for this host.
informs | **traps**	(Optional) Sends SNMP traps or informs to this host.
version 1 | **2c** | **3**	(Optional) Specifies the version of the SNMP used to send the traps. **1—**SNMPv1. This option is not available with informs. **2c—**SNMPv2C. **3—**SNMPv3. One of the authorization keywords (see next table row) must follow the Version 3 keyword.
auth | **noauth** | **priv**	**auth** (Optional)**—**Enables Message Digest 5 (MD5) and Secure Hash Algorithm (SHA) packet authentication. **noauth** (Default)**—**The noAuthNoPriv security level. This is the default if the **auth** | **noauth** | **priv** keyword choice is not specified. **priv** (Optional)**—**Enables Data Encryption Standard (DES) packet encryption (also called privacy).
community-string	Password-like community string sent with the notification operation. Though you can set this string by using the **snmp-server host** command, we recommend that you define this string by using the **snmp-server community** global configuration command before using the **snmp-server host** command. **Note** The @ symbol is used for delimiting the context information. Avoid using the @ symbol as part of the SNMP community string when configuring this command.

notification-type (Optional) Type of notification to be sent to the host. If no type is specified, all notifications are sent. The notification type can be one or more of the these keywords:

- **auth-framework—**Sends SNMP CISCO-AUTH-FRAMEWORK-MIB traps.
- **bridge—**Sends SNMP Spanning Tree Protocol (STP) bridge MIB traps.
- **bulkstat—**Sends Data-Collection-MIB Collection notification traps.
- **call-home—**Sends SNMP CISCO-CALLHOME-MIB traps.
- **cef—**Sends SNMP CEF traps.
- **config—**Sends SNMP configuration traps.
- **config-copy—**Sends SNMP config-copy traps.
- **config-ctid—**Sends SNMP config-ctid traps.
- **copy-config—**Sends SNMP copy configuration traps.
- **cpu—**Sends CPU notification traps.
- **cpu threshold—**Sends CPU threshold notification traps.
- **entity—**Sends SNMP entity traps.

- **envmon—**Sends environmental monitor traps.
- **errdisable—**Sends SNMP errdisable notification traps.
- **event-manager—**Sends SNMP Embedded Event Manager traps.
- **flash—**Sends SNMP FLASH notifications.
- **flowmon—**Sends SNMP flowmon notification traps.
- **ipmulticast—**Sends SNMP IP multicast routing traps.
- **ipsla—**Sends SNMP IP SLA traps.
- **license—**Sends license traps.
- **local-auth—**Sends SNMP local auth traps.
- **mac-notification—**Sends SNMP MAC notification traps.
- **msdp—**Sends SNMP Multicast Source Discovery Protocol (MSDP) traps.
- **pim—**Sends SNMP Protocol-Independent Multicast (PIM) traps.
- **power-ethernet—**Sends SNMP power Ethernet traps.
- **rtr—**Sends SNMP Response Time Reporter traps.
- **snmp—**Sends SNMP-type traps.
- **storm-control—**Sends SNMP storm-control traps.
- **stpx—**Sends SNMP STP extended MIB traps.
- **syslog—**Sends SNMP syslog traps.
- **transceiver—**Sends SNMP transceiver traps.
- **tty—**Sends TCP connection traps.
- **vlan-membership—** Sends SNMP VLAN membership traps.
- **vlancreate—**Sends SNMP VLAN-created traps.
- **vlandelete—**Sends SNMP VLAN-deleted traps.
- **vrfmib—**Sends SNMP vrfmib traps.
- **vtp—**Sends SNMP VLAN Trunking Protocol (VTP) traps.
- **wireless—**Sends wireless traps.

Command Default

This command is disabled by default. No notifications are sent.

If you enter this command with no keywords, the default is to send all trap types to the host. No informs are sent to this host.

If no **version** keyword is present, the default is Version 1.

If Version 3 is selected and no authentication keyword is entered, the default is the **noauth** (noAuthNoPriv) security level.

Note Though visible in the command-line help strings, the **fru-ctrl** keyword is not supported.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. Traps are unreliable because the receiver does not send acknowledgments when it receives traps. The sender cannot determine if the traps were received. However, an SNMP entity that receives an inform request acknowledges the message with an SNMP response PDU. If the sender never receives the response, the inform request can be sent again, so that informs are more likely to reach their intended destinations.

However, informs consume more resources in the agent and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform request must be held in memory until a response is received or the request times out. Traps are also sent only once, but an inform might be retried several times. The retries increase traffic and contribute to a higher overhead on the network.

If you do not enter an **snmp-server host** command, no notifications are sent. To configure the controller to send SNMP notifications, you must enter at least one **snmp-server host** command. If you enter the command with no keywords, all trap types are enabled for the host. To enable multiple hosts, you must enter a separate **snmp-server host** command for each host. You can specify multiple notification types in the command for each host.

If a local user is not associated with a remote host, the controller does not send informs for the **auth** (authNoPriv) and the **priv** (authPriv) authentication levels.

When multiple **snmp-server host** commands are given for the same host and kind of notification (trap or inform), each succeeding command overwrites the previous command. Only the last **snmp-server host** command is in effect. For example, if you enter an **snmp-server host inform** command for a host and then enter another **snmp-server host inform** command for the same host, the second command replaces the first.

The **snmp-server host** command is used with the **snmp-server enable traps** global configuration command. Use the **snmp-server enable traps** command to specify which SNMP notifications are sent globally. For a host to receive most notifications, at least one **snmp-server enable traps** command and the **snmp-server host** command for that host must be enabled. Some notification types cannot be controlled with the **snmp-server enable traps** command. For example, some notification types are always enabled. Other notification types are enabled by a different command.

The **no snmp-server host** command with no keywords disables traps, but not informs, to the host. To disable informs, use the **no snmp-server host informs** command.

Examples

This example shows how to configure a unique SNMP community string named comaccess for traps and prevent SNMP polling access with this string through access-list 10:

```
Controller(config)# snmp-server community comaccess ro 10
Controller(config)# snmp-server host 172.20.2.160 comaccess
Controller(config)# access-list 10 deny any
```

This example shows how to send the SNMP traps to the host specified by the name myhost.cisco.com. The community string is defined as comaccess:

```
Controller(config)# snmp-server enable traps
Controller(config)# snmp-server host myhost.cisco.com comaccess snmp
```

This example shows how to enable the controller to send all traps to the host myhost.cisco.com by using the community string public:

```
Controller(config)# snmp-server enable traps
Controller(config)# snmp-server host myhost.cisco.com public
```

You can verify your settings by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
snmp-server enable traps	Enables the controller to send SNMP notifications for various traps or inform requests to the NMS.

trapflags

To enable trapflags for various parameters, use the **trapflags** command. To disable, use the **no** form of the command.

trapflags {**ap** | {**interfaceup | register**}| **client** | {**dot11 | excluded**}| **dot11-security** | {**ids-sig-attack | wep-decrypt-error**}| **mesh** | **rougeap** | **rrm-params** | {**channels | tx-power**}| **rrm-profile** | {**coverage | interference | load | noise**}}

no trapflags {**ap** | {**interfaceup | register**}| **client** | {**dot11 | excluded**}| **dot11-security** | {**ids-sig-attack | wep-decrypt-error**}| **mesh** | **rougeap** | **rrm-params** | {**channels | tx-power**}| **rrm-profile** | {**coverage | interference | load | noise**}}

Syntax Description

ap	Enables sending of AP-related traps.
interfaceup	Enables the trap when a Cisco AP interface (A or B) comes up.
register	Enables the trap when a Cisco AP registers with a Cisco controller.
client	Enables sending of client-related Dot11 traps.
dot11	Enables dot11 traps for clients.
excluded	Enables excluded traps for clients.
dot11-security	Enables sending of 802.11 security-related traps.
ids-sig-attack	Enables IDS signature attack traps.
wep-decrypt-error	Enables WEP decrypt error for clients.
mesh	Enables mesh trap.
rougeap	Enables rogueAP detection trap.
rrm-params	Enables sending of RRM parameter update-related traps.
channels	Enables trap when RF Manager automatically changes the channel number for the Cisco AP interface.
tx-power	Enables trap when RF Manager automatically changes Tx-Power Level for the Cisco AP interface.
rrm-profile	Enables sending of RRM profile-related traps.
coverage	Enables trap when the coverage profile maintained by RF Manager fails.
interference	Enables trap when the interference profile maintained by RF Manager fails.

load	Enables trap when the load profile maintained by RF Manager fails.
noise	Enables trap when the noise profile maintained by RF Manager fails.

Command Default Disabled

Command Modes Interface configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples This example shows how the trap is enabled for the ids-sig-attach parameter in dot11 security.

```
Controller(config)# trapflags dot11-security ids-sig-attack
```

INDEX

A

B

C

D

E

F

H

I

L

M

N

O

P

Q

R

S

T

U

V

W