QoS Command Reference, Cisco IOS XE 3SE (Cisco WLC 5700 Series)

First Published: January 29, 2013

Last Modified: October 07, 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-28501-02

CONTENTS

Preface

Preface vii

Document Conventions vii

Related Documentation ix

Obtaining Documentation and Submitting a Service Request ix

CHAPTER 1

Using the Command-Line Interface 1

Information About Using the Command-Line Interface 1

Command Modes 1

Using the Help System 3

Understanding Abbreviated Commands 5

No and Default Forms of Commands 5

CLI Error Messages 5

Configuration Logging 6

How to Use the CLI to Configure Features 6

Configuring the Command History 6

Changing the Command History Buffer Size 6

Recalling Commands 7

Disabling the Command History Feature 7

Enabling and Disabling Editing Features 8

Editing Commands Through Keystrokes 9

Editing Command Lines That Wrap 10

Searching and Filtering Output of show and more Commands 11

Accessing the CLI Through a Console Connection or Through Telnet 12

CHAPTER 2

QoS Commands 13

class 15

class-map 18

debug platform qos-acl-tcam 20
debug qos-manager 21
match (access-map configuration) 22
match (class-map configuration) 24
match non-client-nrt 28
match wlan user-priority 29
police 30
policy-map 33
priority-queue 37
priority 39
queue-buffers ratio 41
queue-limit 43
queue-set 45
qos wireless-default untrust 46
service-policy (Wired) 48
service-policy (WLAN) 51
set 53
show ap name service-policy 61
show ap name dot11 62
show class-map 65
show platform qos 66
show platform qos advanced 68
show platform qos dscp-cos counters 70
show platform qos internal table 72
show platform qos policies 73
show platform qos policy 74
show platform qos queue 75
show platform qos trust-data 77
show platform qos wireless 78
show wireless client calls 80
show wireless client dot11 81
show wireless client mac-address (Call Control) 82
show wireless client mac-address (TCLAS) 83
show wireless client voice diagnostics 84
show policy-map 85

show wlan 89

trust 92

trust device 94

Preface

- Document Conventions, page vii
- Related Documentation, page ix
- Obtaining Documentation and Submitting a Service Request, page ix

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.
[x | y]	Optional alternative keywords are grouped in brackets and separated by vertical bars.

Convention	Description
{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 may use 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

- Error Message Decoder, located at:

  https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

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

- Information About Using the Command-Line Interface, page 1
- How to Use the CLI to Configure Features, page 6

Information About Using the Command-Line Interface

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.

You can start a CLI session through a console connection, through Telnet, a SSH, or by using the browser.

When you start a session, 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. Use this mode to execute privilege EXEC commands for access points. These commands are not part of the running config of the controller, they are sent to the IOS config of the access point.
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. Use this mode to configure access point commands that are part of the running config of the controller.
VLAN configuration	While in global configuration mode, enter the **vlan** *vlan-id* command.	`Controller(config-vlan)#`		

Mode	Access Method	Prompt	Exit Method	About This Mode
			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.
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.

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 (?) without any 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 of 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 of 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. This procedure is optional.

SUMMARY STEPS

1. **terminal 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 privileged EXEC mode. You can configure the size from 0 to 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.
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. This procedure is optional.

SUMMARY STEPS

1. **terminal 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 privileged EXEC mode.

Enabling and Disabling Editing Features

Although enhanced editing mode is automatically enabled, you can disable it and reenable it.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**terminal editing** **Example:** `Controller# terminal editing`	Reenables the enhanced editing mode for the current terminal session in privileged EXEC mode.
Step 2	**terminal no editing** **Example:** `Controller# terminal no editing`	Disables the enhanced editing mode for the current terminal session in privileged EXEC 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.

Table 3: Editing Commands

Editing Commands	Description
Ctrl-B or use the **left arrow** key	Moves the cursor back one character.
Ctrl-F or use the **right arrow** key	Moves the cursor forward one character.
Ctrl-A	Moves the cursor to the beginning of the command line.
Ctrl-E	Moves the cursor to the end of the command line.
Esc B	Moves the cursor back one word.
Esc F	Moves the cursor forward one word.
Ctrl-T	Transposes the character to the left of the cursor with the character located at the cursor.
Delete or **Backspace** key	Erases the character to the left of the cursor.
Ctrl-D	Deletes the character at the cursor.
Ctrl-K	Deletes all characters from the cursor to the end of the command line.
Ctrl-U or **Ctrl-X**	Deletes all characters from the cursor to the beginning of the command line.
Ctrl-W	Deletes the word to the left of the cursor.
Esc D	Deletes from the cursor to the end of the word.
Esc C	Capitalizes at the cursor.
Esc L	Changes the word at the cursor to lowercase.
Esc U	Capitalizes letters from the cursor to the end of the word.

Ctrl-V or **Esc Q**	Designates a particular keystroke as an executable command, perhaps as a shortcut.
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.
Space bar	Scrolls down one screen.
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 extends 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`	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

	Command or Action	Purpose

	`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`
		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 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.

QoS Commands

- class, page 15
- class-map, page 18
- debug platform qos-acl-tcam, page 20
- debug qos-manager, page 21
- match (access-map configuration), page 22
- match (class-map configuration), page 24
- match non-client-nrt, page 28
- match wlan user-priority, page 29
- police, page 30
- policy-map, page 33
- priority-queue, page 37
- priority, page 39
- queue-buffers ratio, page 41
- queue-limit, page 43
- queue-set, page 45
- qos wireless-default untrust, page 46
- service-policy (Wired), page 48
- service-policy (WLAN), page 51
- set, page 53
- show ap name service-policy, page 61
- show ap name dot11, page 62
- show class-map, page 65
- show platform qos, page 66
- show platform qos advanced, page 68

- show platform qos dscp-cos counters, page 70
- show platform qos internal table, page 72
- show platform qos policies, page 73
- show platform qos policy, page 74
- show platform qos queue, page 75
- show platform qos trust-data, page 77
- show platform qos wireless, page 78
- show wireless client calls, page 80
- show wireless client dot11, page 81
- show wireless client mac-address (Call Control), page 82
- show wireless client mac-address (TCLAS), page 83
- show wireless client voice diagnostics, page 84
- show policy-map, page 85
- show wlan, page 89
- trust, page 92
- trust device, page 94

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	The class map name.
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 the policy-map class configuration mode. These configuration commands are available:

- **admit—**Admits a request for Call Admission Control (CAC)
- **bandwidth—**Specifies the bandwidth allocated to the class.
- **exit—**Exits the policy-map class configuration mode and returns to policy-map configuration mode.
- **netflow-sampler —**Specifies NetFlow action.
- **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 about this command, see *Cisco IOS Quality of Service Solutions Command Reference* available on Cisco.com.
- **priority—**Assigns scheduling priority to a class of traffic belonging to a policy map.
- **queue-buffers—**Configures the queue buffer for the class.

- **queue-limit—**Specifies the maximum number of packets the queue can hold for a class policy configured in a policy map.
- **service-policy—**Configures a QoS service policy.
- **set—**Specifies a value to be assigned to the classified traffic. For more information, see set, on page 53
- **shape—**Specifies average or peak rate traffic shaping. For more information about this command, see *Cisco IOS Quality of Service Solutions Command Reference* available on Cisco.com.
- **trust—**Defines a trust state for traffic classified with the **class** or the **class-map** command. For more information, see trust, on page 92.

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.

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

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

```
Controller# configure terminal
Controller(config)# class-map cm-3
Controller(config-cmap)# match ip dscp 30
Controller(config-cmap)# exit

Controller(config)# class-map cm-4
Controller(config-cmap)# match ip dscp 40
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)# set precedence 5
```

```
Controller(config-pmap-c)# exit
Controller(config-pmap)# exit

Controller# show policy-map pm3
Policy Map pm3
  Class cm-3
    set dscp 4
  Class cm-4
    set precedence 5
  Class class-default
    set dscp af11
```

Related Commands

class-map, on page 18	Creates a class map to be used for matching packets to the class whose name you specify.
police, on page 30	Defines a policer for classified traffic.
policy-map, on page 33	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
set, on page 53	Classifies IP traffic by setting a DSCP or IP-precedence value in the packet.
show policy-map, on page 85	Displays quality of service (QoS) policy maps.
trust, on page 92	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.
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.
set	Classifies IP traffic by setting a DSCP or an IP-precedence value in the packet.

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**| *type*] *class-map-name*

no class-map [**match-any**| *type*] *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.
type	(Optional) Configures the CPL class map.
class-map-name	The class map name.

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.
Cisco IOS XE 3.3SE	The **type** keyword was added.

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 24 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
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.

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*}| **class-map** *class-map-name*| **cos** *cos-value*| **dscp** *dscp-value*| **[ip] dscp** *dscp-list* | **[ip] precedence** *ip-precedence-list*| **precedence** *precedence-value1...value4*| **qos-group** *qos-group-value*| **vlan** *vlan-id*}

no match {**access-group**{**name***acl-name* | *acl-index*}| **class-map** *class-map-name*| **cos** *cos-value*| **dscp** *dscp-value*| **[ip] dscp** *dscp-list* | **[ip] precedence** *ip-precedence-list*| **precedence** *precedence-value1...value4*| **qos-group** *qos-group-value*| **vlan** *vlan-id*}

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	Specifies an access group.
name *acl-name*	Specifies the name of an IP standard or extended access control list (ACL) or MAC ACL.
acl-index	Specifies 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.
class-map *class-map-name*	Uses a traffic class as a classification policy and specifies a traffic class name to use as the match criterion.
cos *cos-value*	Matches a packet on the basis of a Layer 2 class of service (CoS)/Inter-Switch Link (ISL) marking. The cos-value is from 0 to 7. You can specify up to four CoS values in one **match cos** statement, separated by a space.
dscp *dscp-value*	Specifies the parameters for each DSCP value. You can specify a value in the range 0 to 63 specifying the differentiated services code point value.
ip dscp *dscp-list*	Specifies a 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*	Specifies a 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.
precedence *precedence-value1...value4*	Assigns an IP precedence value 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*	Identifies a specific QoS group value as a match criterion. The range is 0 to 31.
vlan *vlan-id*	Identifies a specific VLAN as a match criterion. The range is 1 to 4095.

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.
Cisco IOS XE 3.3SE	The **class-map** *class-map-name*, **cos** *cos-value*, **qos-group** *qos-group-value*, and **vlan** *vlan-id* keywords were added.

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*

The **match access-group** *acl-index* command is not supported.

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-any class4
Controller(config-cmap)# match cos 4
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-any class4
Controller(config-cmap)# match cos 4
Controller(config-cmap)# exit
```

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

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

This example show how you can configure non-client NRT:

```
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** 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	The 802.11-specific values. Enter the user priority 802.11 TID user priority (0-7). (Optional) Enter up to three 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

This example show how you can configure user-priority values:

```
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 18	Create a class map to be used for matching packets to the class whose name you specify with the **class** command.
class, on page 15	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 33	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.

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.

A hierarchical policy map has two levels in the format of a parent-child policy. The parent policy cannot be modified but the child policy (port-child policy) can be modified to suit the QoS configuration.

In VLAN-based QoS, a service policy is applied to an SVI interface. All physical interfaces belonging to a VLAN policy map then need to be configured to refer to the VLAN-based policy maps instead of the port-based policy map.

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)*.

Note Not all MQC QoS combinations are supported for wired and wireless ports. For information about these restrictions, see chapters "Restrictions for QoS on Wired Targets" and "Restrictions for QoS on Wireless Targets" in the QoS configuration guide.

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 show you how to configure hierarchical polices:

```
Switch# configure terminal
Controller(config)# class-map c1
Controller(config-cmap)# exit

Controller(config)# class-map c2
Controller(config-cmap)# exit

Controller(config)# policy-map child
Controller(config-pmap)# class c1
```

```
Controller(config-pmap-c)# priority level 1
Controller(config-pmap-c)# police rate percent 20 conform-action transmit exceed action
drop
Controller(config-pmap-c-police)# exit
Controller(config-pmap-c)# exit

Controller(config-pmap)# class c2
Controller(config-pmap-c)# bandwidth 20000
Controller(config-pmap-c)# exit

Controller(config-pmap)# class class-default
Controller(config-pmap-c)# bandwidth 20000
Controller(config-pmap-c)# exit
Controller(config-pmap)# exit

Controller(config)# policy-map parent
Controller(config-pmap)# class class-default
Controller(config-pmap-c)# shape average 1000000
Controller(config-pmap-c)# service-policy child
Controllerconfig-pmap-c)# end
```

This example shows how to delete a policy map:

```
Controller(config)# no policy-map policymap2
```

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

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 exceeding the profile is marked down to a DSCP value received 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 multiple classes in a policy map called *policymap2*:

```
Controller(config)# policy-map policymap2
Controller(config-pmap)# class class1
Controller(config-pmap-c)# set dscp 10
Controller(config-pmap-c)# police 100000 20000 exceed-action policed-dscp-transmit
Controller(config-pmap-c)# exit
Controller(config-pmap)# class class2
Controller(config-pmap-c)# trust dscp
Controller(config-pmap-c)# police 100000 20000 exceed-action drop
Controller(config-pmap-c)# exit
Controller(config-pmap)# class class3
Controller(config-pmap-c)# set dscp 0
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
```

Related Commands

Command	Description
class, on page 15	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 18	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 (Wired)	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 [*Kbps* [*burst -in-bytes*] | **level** *level-value* [*Kbps* [*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

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 the burst 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 the bandwidth even if you do not use it. Both levels 1 and 2 can reserve bandwidth.
percent *percentage*	(Optional) Specifies the amount of guaranteed bandwidth to 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.
Cisco IOS XE 3.3SE	The *Kbps*, *burst -in-bytes*, and **percent** *percentage* keywords were added.

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.

Note You can configure a priority only with a level.
Only one strict priority or priority with levels is allowed in one policy-map. Multiple priorities with same priority levels without kbps/percent are allowed in a policy-map only if all of them are configured with police.

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. However, these commands can be used together in the same policy map.

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.

Examples

The following example shows how to configure the priority of the class in policy map policy1:

```
Controller(config)# class-map cm1
Controller(config-cmap)#match precedence 2
Controller(config-cmap)#exit

Controller(config)#class-map cm2
Controller(config-cmap)#match dscp 30
Controller(config-cmap)#exit

Controller(config)# policy-map policy1
Controller(config-pmap)# class cm1
Controller(config-pmap-c)# priority level 1
Controller(config-pmap-c)# police 1m
Controller(config-pmap-c-police)#exit
Controller(config-pmap-c)#exit
Controller(config-pmap)#exit

Controller(config)#policy-map policy1
Controller(config-pmap)#class cm2
Controller(config-pmap-c)#priority level 2
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 the **bandwidth**, **shape**, or **priority** command must be used before using this command. For more information about these commands, see *Cisco IOS Quality of Service Solutions Command Reference* available on Cisco.com

The controller allows you to allocate buffers to queues. If buffers are not allocated, then they are divided equally amongst all queues. You can use the queue-buffer ratio to divide it in a particular ratio. The buffers are soft buffers because Dynamic Threshold and Scaling (DTS) is active on all queues by default.

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 percent:

```
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.

Related Commands

Command	Description
show policy-map	Displays QoS policy maps.

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 *queue-limit-size* [**packets**] {**cos** *cos-value*| **dscp** *dscp-value*} **percent** *percentage-of-packets*

no queue-limit *queue-limit-size* [**packets**] {**cos** *cos-value*| **dscp** *dscp-value*} **percent** *percentage-of-packets*

Syntax Description

queue-limit-size	The maximum size of the queue. The maximum varies according to the optional unit of measure keyword specified (bytes, ms, us, or packets).
cos *cos-value*	Specifies parameters for each cos value. CoS values are from 0 to 7.
dscp *dscp-value*	Specifies parameters for each DSCP value. You can specify a value in the range 0 to 63 specifying the differentiated services code point value for the type of queue limit .
percent *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

Although visible in the command line help-strings, the **packets** unit of measure is not supported; use the **percent** unit of measure.

Note This command is supported only on wired ports in the egress direction.

Weighted fair queuing (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 queuing process. When the maximum packet threshold you defined for the class is reached, queuing 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.

You can configure the maximum queue thresholds for the different subclasses of traffic, that is, DSCPprecedence and CoS and configure the maximum queue thresholds for each subclass.

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 percent:

```
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	Queue-set ID. 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.

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.

qos wireless-default untrust

To configure the default trust behavior to untrust wireless packets, use the **qos wireless-default untrust** command. To configure the default trust behavior of wireless traffic to trust, use the **no** form of the command.

qos wireless-default-untrust

no qos wireless-default-untrust

Syntax Description

This command has no arguments or keywords.

Command Default

By default, the wireless traffic is untrusted.

To check the trust behavior on the controller, use the **show running-config** | **sec qos** or the **show run** | **include untrust** command.

Command Modes

Configuration

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

Usage Guidelin

Note The default trust behavior of wireless traffic was untrusted in the Cisco IOS XE 3.2 SE release.

Note If you upgrade from Cisco IOS XE 3.2 SE Release to a later release, the default behavior of the wireless traffic is still untrusted. In this situation, you can use the **no qos wireless-default untrust** command to enable trust behavior for wireless traffic. However, if you install Cisco IOS XE 3.3 SE or a later release on the controller, the default QoS behavior for wireless traffic is trust. Starting with Cisco IOS XE 3.3 SE Release and later, the packet markings are preserved in both egress and ingress directions for new installations (not upgrades) for wireless traffic.

The Cisco IOS XE 3.2 Release supported different trust defaults for wired and wireless ports. The trust default for wired ports was the same as for this software release. For wireless ports, the default system behavior was non-trust, which meant that when the controller came up, all markings for the wireless ports were defaulted to zero and no traffic received priority treatment. For compatibility with an existing wired controller, all traffic went to the best-effort queue by default. The access point performed priority queuing by default. In the downstream direction, the access point maintained voice, video, best-effort, and background queues for queuing. The access selected the queuing strategy based on the 11e tag information. By default, the access point treated all wireless packets as best effort.

Examples The following command changes the default behavior for trusting wireless traffic to untrust.

```
Controller(config)# qos wireless-default-untrust
```

service-policy (Wired)

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

WLAN 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 85	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	The policy name.

Command Default

No policies are assigned and the state assigned to the policy is None.

Command Modes

WLAN 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. See Related Commands section for more information on how to disable a WLAN.

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
```

This example shows how to configure the output QoS service policy on a WLAN to platinum (precious metal policy):

```
Controller# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

```
Controller(config)# wlan wlan1
Controller(config-wlan)# service-policy output platinum
```

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 cos| dscp| precedence| ip| qos-group| wlan

set cos {*cos-value* } | {**cos| dscp| precedence| qos-group| wlan**} [**table** *table-map-name*]

set dscp {*dscp-value* } | {**cos| dscp| precedence| qos-group| wlan**} [**table** *table-map-name*]

set ip {**dscp| precedence**}

set precedence {*precedence-value* } | {**cos| dscp| precedence| qos-group**} [**table** *table-map-name*]

set qos-group {*qos-group-value*| **dscp** [**table** *table-map-name*]| **precedence** [**table** *table-map-name*]}

set wlan user-priority*user-priority-value*| **costable** *table-map-name*| **dscptable** *table-map-name*| **qos-grouptable** *table-map-name*| **wlantable** *table-map-name*

Syntax Description

cos	Sets the Layer 2 class of service (CoS) value or user priority of an outgoing packet. You can specify these values: • *cos-value*—CoS value from 0 to 7. You also can enter a mnemonic name for a commonly used value. • Specify a packet-marking category to set the CoS value of the packet. If you also configure a table map for mapping and converting packet-marking values, this establishes the "map from" packet-marking category. Packet-marking category keywords: ◦ **cos**—Sets a value from the CoS value or user priority. ◦ **dscp**—Sets a value from packet differentiated services code point (DSCP). ◦ **precedence**—Sets a value from packet precedence. ◦ **qos-group**—Sets a value from the QoS group. ◦ **wlan**—Sets the WLAN user priority values. • (Optional)**table** *table-map-name*—Indicates that the values set in a specified table map are used to set the CoS value. Enter the name of the table map used to specify the CoS value. The table map name can be a maximum of 64 alphanumeric characters. If you specify a packet-marking category but do not specify the table map, the default action is to copy the value associated with the packet-marking category as the CoS value. For example, if you enter the **set cos precedence** command, the precedence (packet-marking category) value is copied and used as the CoS value.

dscp	Sets the differentiated services code point (DSCP) value to mark IP(v4) and IPv6 packets. You can specify these values: • *cos-value*—Number that sets the DSCP value. The range is from 0 to 63. You also can enter a mnemonic name for a commonly used value. • Specify a packet-marking category to set the DSCP value of the packet. If you also configure a table map for mapping and converting packet-marking values, this establishes the "map from" packet-marking category. Packet-marking category keywords: ◦ **cos**—Sets a value from the CoS value or user priority. ◦ **dscp**—Sets a value from packet differentiated services code point (DSCP). ◦ **precedence**—Sets a value from packet precedence. ◦ **qos-group**—Sets a value from the QoS group. ◦ **wlan**—Sets a value from WLAN. • (Optional)**table** *table-map-name*—Indicates that the values set in a specified table map will be used to set the DSCP value. Enter the name of the table map used to specify the DSCP value. The table map name can be a maximum of 64 alphanumeric characters. If you specify a packet-marking category but do not specify the table map, the default action is to copy the value associated with the packet-marking category as the DSCP value. For example, if you enter the **set dscp cos** command, the CoS value (packet-marking category) is copied and used as the DSCP value.
ip	Sets IP values to the classified traffic. You can specify these values: • **dscp**—Specify an IP DSCP value from 0 to 63 or a packet marking category. • **precedence**—Specify a precedence-bit value in the IP header; valid values are from 0 to 7 or specify a packet marking category.

precedence	Sets the precedence value in the packet header. You can specify these values: • *precedence-value*— Sets the precedence bit in the packet header; valid values are from 0 to 7. You also can enter a mnemonic name for a commonly used value. • Specify a packet marking category to set the precedence value of the packet. ◦ **cos**—Sets a value from the CoS or user priority. ◦ **dscp**—Sets a value from packet differentiated services code point (DSCP). ◦ **precedence**—Sets a value from packet precedence. ◦ **qos-group**—Sets a value from the QoS group. • (Optional)**table** *table-map-name*—Indicates that the values set in a specified table map will be used to set the precedence value. Enter the name of the table map used to specify the precedence value. The table map name can be a maximum of 64 alphanumeric characters. If you specify a packet-marking category but do not specify the table map, the default action is to copy the value associated with the packet-marking category as the precedence value. For example, if you enter the **set precedence cos** command, the CoS value (packet-marking category) is copied and used as the precedence value.

qos-group	Assigns a QoS group identifier that can be used later to classify packets. • *qos-group-value*—Sets a QoS value to the classified traffic. The range is 0 to 31. You also can enter a mnemonic name for a commonly used value. • **dscp**—Sets the original DSCP field value of the packet as the QoS group value. • **precedence**—Sets the original precedence field value of the packet as the QoS group value. • (Optional)**table** *table-map-name*—Indicates that the values set in a specified table map will be used to set the DSCP or precedence value. Enter the name of the table map used to specify the value. The table map name can be a maximum of 64 alphanumeric characters. If you specify a packet-marking category (**dscp** or **precedence**) but do not specify the table map, the default action is to copy the value associated with the packet-marking category as the QoS group value. For example, if you enter the **set qos-group precedence** command, the precedence value (packet-marking category) is copied and used as the QoS group value.

wlan user-priority *wlan-user-priority*	Assigns a WLAN user-priority to the classified traffic. You can specify these values: • *wlan-user-priority*—Sets a WLAN user priority to the classified traffic. The range is 0 to 7. • **cos**—Sets the Layer 2 CoS field value as the WLAN user priority. • **dscp**—Sets the DSCP field value as the WLAN user priority. • **precedence**—Sets the precedence field value as the WLAN user priority. • **wlan**—Sets the WLAN user priority field value as the WLAN user priority. • (Optional)**table** *table-map-name*—Indicates that the values set in a specified table map will be used to set the WLAN user priority value. Enter the name of the table map used to specify the value. The table map name can be a maximum of 64 alphanumeric characters. If you specify a packet-marking category but do not specify the table map, the default action is to copy the value associated with the packet-marking category as the WLAN user priority. For example, if you enter the **set wlan user-priority cos** command, the cos value (packet-marking category) is copied and used as the WLAN user priority.

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.
Cisco IOS XE 3.3SE	The **cos**, **dscp**, **qos-group**, **wlantable** *table-map-name*, keywords were added.

Usage Guidelines

For the **set dscp** *dscp-value* command, the **set cos** *cos-value* command, and the **set ip precedence** *precedence-value* 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.

When you configure the **set dscp cos**command, note the following: The CoS value is a 3-bit field, and the DSCP value is a 6-bit field. Only the three bits of the CoS field are used.

When you configure the **set dscp qos-group** command, note the following:

- The valid range for the DSCP value is a number from 0 to 63. The valid value range for the QoS group is a number from 0 to 99.
- If a QoS group value falls within both value ranges (for example, 44), the packet-marking value is copied and the packets is marked.
- If QoS group value exceeds the DSCP range (for example, 77), the packet-marking value is not be copied and the packet is not marked. No action is taken.

The **set qos-group** command cannot be applied until you create a service policy in policy-map configuration mode and then attach the service policy to an interface or ATM virtual circuit (VC).

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 85	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.
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.

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) The class map name.

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-any 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-any 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.

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.

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
---------       ------  ---------       ------  ------
R43761937175019671      def-11an        OUT     0x009b794000000097      INSTALLED IN HW
R53644897441284244      def-11an        OUT     0x00be95c000000094      INSTALLED IN HW
R48977470581375121      def-11an        OUT     0x00ae00c000000091      INSTALLED IN HW
R44668759390027918      def-11an        OUT     0x009eb2000000008e      INSTALLED IN HW
R44353749308670091      def-11an        OUT     0x009d93800000008b      INSTALLED IN HW
R50434323488178312      def-11an        OUT     0x00b32dc000000088      INSTALLED IN HW
R47286421697855621      def-11an        OUT     0x00a7fec000000085      INSTALLED IN HW
R38541181088432258      def-11an        OUT     0x0088ed0000000082      INSTALLED IN HW
R44458752669122687      def-11an        OUT     0x009df3000000007f      INSTALLED IN HW
R52212783546105980      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 in privileged EXEC mode.

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

Syntax Description

active	Displays active calls.
rejected	Displays rejected calls.

Command Default

No default behavior or values.

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 in privileged EXEC mode.

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

No default behavior or values.

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 in privileged EXEC mode.

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 voice diagnostics that are enabled for TSPEC clients.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

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

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*| **interface** *interface-id*]

Syntax Description

policy-map-name	(Optional) Name of the policy-map.
interface *interface-id*	(Optional) Identifies the interface.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.
Cisco IOS XE 3.3SE	The **interface** *interface-id* keyword was added.

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**, **session**, and **type** keywords are not supported, and the statistics shown in the display should be ignored.

To display classification counters for ternary content addressable memory (TCAM) (marking or policing) based policies, enter the interface ID. Classification counters have the following restrictions:

- Classification counters are supported only on wired ports (in the ingress and egress directions).
- Classification counters count packets instead of bytes.
- Only QoS configurations with marking or policing trigger the classification counter.
- As long as there is policing or marking action in the policy, the class-default will have classification counters.
- Classification counters are not port based. The counters are shared across targets sharing the same policy map. This means that the classification counter aggregates all packets belonging to the same class of the same policy which attach to different interfaces.

Examples

This is an example of output from the **show policy-map interface** command, where classification counters are displayed:

```
Controller# show policy-map interface gigabitethernet1/0/1

  GigabitEthernet1/0/1

  Service-policy input: AutoQos-4.0-CiscoPhone-Input-Policy

    Class-map: AutoQos-4.0-Voip-Data-CiscoPhone-Class (match-any)
      0 packets
      Match: cos  5
        0 packets, 0 bytes
        5 minute rate 0 bps
      QoS Set
        dscp ef
      police:
          cir 128000 bps, bc 8000 bytes
        conformed 0 bytes; actions:
          transmit
        exceeded 0 bytes; actions:
          set-dscp-transmit dscp table policed-dscp
        conformed 0000 bps, exceed 0000 bps

    Class-map: AutoQos-4.0-Voip-Signal-CiscoPhone-Class (match-any)
      0 packets
      Match: cos  3
        0 packets, 0 bytes
        5 minute rate 0 bps
      QoS Set
        dscp cs3
      police:
          cir 32000 bps, bc 8000 bytes
        conformed 0 bytes; actions:
          transmit
        exceeded 0 bytes; actions:
          set-dscp-transmit dscp table policed-dscp
        conformed 0000 bps, exceed 0000 bps

    Class-map: AutoQos-4.0-Default-Class (match-any)
      0 packets
      Match: access-group name AutoQos-4.0-Acl-Default
        0 packets, 0 bytes
        5 minute rate 0 bps
      QoS Set
        dscp default

    Class-map: class-default (match-any)
      0 packets
      Match: any
        0 packets, 0 bytes
        5 minute rate 0 bps

  Service-policy output: AutoQos-4.0-Output-Policy

    queue stats for all priority classes:
      Queueing
      priority level 1

      (total drops) 0
      (bytes output) 0

    Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
      0 packets
      Match:  dscp cs4 (32) cs5 (40) ef (46)
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: cos  5
        0 packets, 0 bytes
        5 minute rate 0 bps
```

```
  Priority: 30% (300000 kbps), burst bytes 7500000,

  Priority Level: 1

Class-map: AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
  0 packets
  Match:  dscp cs2 (16) cs3 (24) cs6 (48) cs7 (56)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  3
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing
  queue-limit dscp 16 percent 80
  queue-limit dscp 24 percent 90
  queue-limit dscp 48 percent 100
  queue-limit dscp 56 percent 100

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%

  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
  0 packets
  Match:  dscp af41 (34) af42 (36) af43 (38)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  4
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Trans-Data-Queue (match-any)
  0 packets
  Match:  dscp af21 (18) af22 (20) af23 (22)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  2
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
  0 packets
  Match:  dscp af11 (10) af12 (12) af13 (14)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  1
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 4%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
  0 packets
  Match:  dscp cs1 (8)
    0 packets, 0 bytes
```

```
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 1%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)
  0 packets
  Match:  dscp af31 (26) af32 (28) af33 (30)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: class-default (match-any)
  0 packets
  Match: any
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 25%
  queue-buffers ratio 25
```

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.

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 *wlan-id*	Specifies the wireless LAN identifier. The range is from 1 to 512.
name *wlan-name*	Specifies the 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 name 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
WifiDirect                                      : Disabled
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
-----------
```

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	Configures a Cisco IP phone
cts	Configures a Cisco TelePresence System
ip-camera	Configures an IP Video Surveillance Camera (IPVSC)
media-player	Configures a Cisco Digital 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—** auto-template interface
- **Capwap—**CAPWAP tunnel interface
- **GigabitEthernet—**Gigabit Ethernet IEEE 802
- **GroupVI—**Group virtual interface
- **Internal Interface—**Internal interface
- **Loopback—**Loopback interface
- **Null—**Null interface
- **Port-channel—**Ethernet Channel interface
- **TenGigabitEthernet--**10-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.

INDEX

C

class command 15
class-map command 18

D

debug platform qos-acl-tcam command 20
debug qos-manager command 21

M

match (access-map configuration) command 22
match (class-map configuration) command 24
match non-client-nrt command 28
match wlan user-priority command 29

P

police command 30
policy-map command 33
priority-queue command 37

Q

queue-limit command 43
queue-set command 45

S

service-policy command 48, 51
set command 53
show ap name dot11 62
show ap name service-policy 61
show class-map command 65
show platform qos advanced command 68
show platform qos command 66
show platform qos dscp-cos counters command 70
show platform qos internal table command 72
show platform qos policies command 73
show platform qos policy command 74
show platform qos queue command 75
show platform qos trust-data command 77
show platform qos wireless command 78
show policy-map command 85
show wireless client calls command 80
show wireless client dot11 command 81
show wireless client mac-address command 82, 83
show wireless client voice diagnostics command 84
show wlan command 89

T

trust command 92