Catalyst 2960-X Switch QoS Command Reference, Cisco IOS Release 15.0(2)EX

First Published: July 10, 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-29047-01

CONTENTS

Preface

This preface contains the following topics:

Document Conventions

This document uses the following conventions:

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

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

Reader Alert Conventions

This document uses the following conventions for reader alerts:

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

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

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

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

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

Related Documentation

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

- Catalyst 2960-X Switch documentation, located at:

  http://www.cisco.com/go/cat2960x_docs

- Cisco SFP and SFP+ modules documentation, including compatibility matrixes, located at:

  http://www.cisco.com/en/US/products/hw/modules/ps5455/tsd_products_support_series_home.html

- Cisco Validated Designs documents, located at:

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

Obtaining Documentation and Submitting a Service Request

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

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

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

Using the Command-Line Interface

This chapter contains the following topics:

Information About Using the Command-Line Interface

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

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 switch 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 switch 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.	`Switch>`	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.	`Switch#`	Enter **disable** to exit.	Use this mode to verify commands that you have entered. Use a password to protect access to this mode.
Global configuration	While in privileged EXEC mode, enter the **configure** command.	`Switch(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 switch.
VLAN configuration	While in global configuration mode, enter the **vlan** *vlan-id* command.	`Switch(config-vlan)#`	To exit to global configuration mode, enter the **exit** command. To return to privileged EXEC mode, press **Ctrl-Z** or enter **end**.	Use this mode to configure VLAN parameters. When VTP mode is transparent, you can create extended-range VLANs (VLAN IDs greater than 1005) and save configurations in the switch startup configuration file.
Interface configuration	While in global configuration mode, enter the **interface** command (with a specific interface).	`Switch(config-if)#`	To exit to global configuration mode, enter **exit**. To return to privileged EXEC mode, press **Ctrl-Z** or enter **end**.	Use this mode to configure parameters for the Ethernet ports.

Mode	Access Method	Prompt	Exit Method	About This Mode
Line configuration	While in global configuration mode, specify a line with the **line vty** or **line console** command.	`Switch(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:** `Switch# help`	Obtains a brief description of the help system in any command mode.

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

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

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

Step 6	*command keyword* **?**
	
	Example:
	`Switch(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 switch to recognize the command as unique.

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

```
Switch# 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 switch.

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 switch to recognize the command.	Reenter the command followed by a question mark (?) with a space between the command and the question mark. The possible keywords that you can enter with the command appear.
`% Incomplete command.`	You did not enter all the keywords or values required by this command.	Reenter the command followed by a question mark (?) with a space between the command and the question mark. The possible keywords that you can enter with the command appear.
`% Invalid input detected at '^' marker.`	You entered the command incorrectly. The caret (^) marks the point of the error.	Enter a question mark (?) to display all the commands that are available in this command mode. The possible keywords that you can enter with the command appear.

Configuration Logging

You can log and view changes to the switch 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 switch 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:** `Switch# terminal history size 200`	Changes the number of command lines that the switch records during the current terminal session in the privileged EXEC mode. You can configure the size from 0 through 256.

Recalling Commands

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

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

SUMMARY STEPS

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

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	**show history** **Example:** `Switch# 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:** `Switch# terminal no history`	Disables the feature during the current terminal session in the 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:** `Switch# terminal editing`	Reenables the enhanced editing mode for the current terminal session in the privileged EXEC mode.

	Command or Action	Purpose
Step 2	**terminal no editing** **Example:** `Switch# terminal no editing`	Disables the enhanced editing mode for the current terminal session in the 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 switch suddenly sends a message to your screen.

Editing Command Lines That Wrap

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

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

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

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**access-list** **Example:** `Switch(config)# access-list 101 permit tcp`	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
	10.15.22.25 255.255.255.0 10.15.22.35 Switch(config)# $ **101 permit tcp 10.15.22.25 255.255.255.0 10.15.22.35 255.25** Switch(config)# $**t tcp 10.15.22.25 255.255.255.0 131.108.1.20 255.255.255.0 eq** Switch(config)# $**15.22.25 255.255.255.0 10.15.22.35 255.255.255.0 eq 45**	line has been scrolled to the left. Each time the cursor reaches the end of the line, the line is again shifted ten spaces to the left.
Step 2	**Ctrl-A** **Example:** Switch(config)# **access-list 101 permit tcp 10.15.22.25 255.255.255.0 10.15.2$**	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:** Switch# **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 switch console or connect a PC to the Ethernet management port and then power on the switch, as described in the hardware installation guide that shipped with your switch.

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

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

- Connect the switch 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 switch hardware installation guide.
- Use any Telnet TCP/IP or encrypted Secure Shell (SSH) package from a remote management station. The switch must have network connectivity with the Telnet or SSH client, and the switch must have an enable secret password configured.
    - The switch supports up to 16 simultaneous Telnet sessions. Changes made by one Telnet user are reflected in all other Telnet sessions.
    - The switch 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.

Auto-QoS Commands

This chapter contains the following auto-QoS commands:

auto qos classify

To automatically configure quality of service (QoS) classification for untrusted devices within a QoS domain, use the **auto qos classify** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

auto qos classify [police]

no auto qos classify [police]

Syntax Description

police	(Optional) Configures QoS policing for untrusted devices.

Command Default

Auto-QoS classify is disabled on the port.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS 15.0(2)EX	This command was introduced.

Usage Guidelines

Use this command to configure the QoS for trusted interfaces within the QoS domain. The QoS domain includes the switch, the network interior, and edge devices that can classify incoming traffic for QoS.

When auto-QoS is enabled, it uses the ingress packet label to categorize traffic, to assign packet labels, and to configure the ingress and egress queues.

Table 4: Auto-QoS Configuration for the Egress Queues

Egress Queue	Queue Number	CoS-to-Queue Map	Queue Weight (Bandwidth)	Queue (Buffer) Size for Gigabit-Capable Ports	Queue (Buffer) Size for 10/100 Ethernet Ports
Priority (shaped)	1	4, 5	up to 100 percent	15 percent	15 percent
SRR shared	2	2, 3, 6,7	10 percent	25 percent	25 percent
SRR shared	3	0	60 percent	40 percent	40 percent
SRR shared	4	1	20 percent	20 percent	20 percent

Auto-QoS configures the switch for connectivity with a trusted interface. The QoS labels of incoming packets are trusted. For nonrouted ports, the CoS value of the incoming packets is trusted. For routed ports, the DSCP value of the incoming packet is trusted.

To take advantage of the auto-QoS defaults, you should enable auto-QoS before you configure other QoS commands. You can fine-tune the auto-QoS configuration *after* you enable auto-QoS.

To display the QoS configuration that is automatically generated when auto-QoS is enabled, enable debugging before you enable auto-QoS. Use the **debug auto qos** privileged EXEC command to enable auto-QoS debugging.

This is the policy map when the **auto qos classify** command is configured:

```
policy-map AUTOQOS-SRND4-CLASSIFY-POLICY
class AUTOQOS_MULTIENHANCED_CONF_CLASS
set dscp af41
class AUTOQOS_BULK_DATA_CLASS
set dscp af11
class AUTOQOS_TRANSACTION_CLASS
set dscp af21
class AUTOQOS_SCAVANGER_CLASS
set dscp cs1
class AUTOQOS_SIGNALING_CLASS
set dscp cs3
class AUTOQOS_DEFAULT_CLASS
set dscp default
```

This is the policy map when the **auto qos classify police** command is configured:

```
policy-map AUTOQOS-SRND4-CLASSIFY-POLICE-POLICY
class AUTOQOS_MULTIENHANCED_CONF_CLASS
set dscp af41
police 5000000 8000 exceed-action drop
class AUTOQOS_BULK_DATA_CLASS
set dscp af11
police 10000000 8000 exceed-action policed-dscp-transmit
class AUTOQOS_TRANSACTION_CLASS
set dscp af21
police 10000000 8000 exceed-action policed-dscp-transmit
class AUTOQOS_SCAVANGER_CLASS
set dscp cs1
police 10000000 8000 exceed-action drop
class AUTOQOS_SIGNALING_CLASS
set dscp cs3
police 32000 8000 exceed-action drop
class AUTOQOS_DEFAULT_CLASS
set dscp default
police 10000000 8000 exceed-action policed-dscp-transmit
```

Note The switch applies the auto-QoS-generated commands as if the commands were entered from the command-line interface (CLI). An existing user configuration can cause the application of the generated commands to fail or to be overridden by the generated commands. These actions occur without warning. If all the generated commands are successfully applied, any user-entered configuration that was not overridden remains in the running configuration. Any user-entered configuration that was overridden can be retrieved by reloading the switch without saving the current configuration to memory. If the generated commands fail to be applied, the previous running configuration is restored.

After auto-QoS is enabled, do not modify a policy map or aggregate policer that includes *AutoQoS* in its name. If you need to modify the policy map or aggregate policer, make a copy of it, and change the copied policy map or policer. To use the new policy map instead of the generated one, remove the generated policy map from the interface and apply the new policy map.

Note To disable auto-QoS, you need remove the auto-QoS commands manually.

Enter the **no mls qos** global configuration command to disable the auto-QoS-generated global configuration commands. With QoS disabled, there is no concept of trusted or untrusted ports because the packets are not modified. The CoS, DSCP, and IP precedence values in the packet are not changed. Traffic is switched in pass-through mode. Packets are switched without any rewrites and classified as best effort without any policing.

To disable auto-QoS on a port, use the **no auto qos trust** interface configuration command. Only the auto-QoS-generated interface configuration commands for this port are removed. If this is the last port on which auto-QoS is enabled and you enter the **no auto qos trust** command, auto-QoS is considered disabled even though the auto-QoS-generated global configuration commands remain (to avoid disrupting traffic on other ports affected by the global configuration).

Examples

This example shows how to enable auto-QoS classification of an untrusted device and police traffic:

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# auto qos classify police
```

You can verify your settings by entering the **show auto qos interface** *interface-id* privileged EXEC command.

Related Commands

Command	Description
debug auto qos, on page 31	Enables debugging of the auto-QoS feature.
mls qos trust, on page 73	Configures the port trust state.
queue-set, on page 82	Maps a port to a queue-set.
show auto qos, on page 34	Displays auto-QoS information.
show mls qos interface, on page 91	Displays QoS information at the port level.
srr-queue bandwidth share, on page 104	Assigns the shared weights and enables bandwidth sharing on the four egress queues mapped to a port.

auto qos trust

To automatically configure quality of service (QoS) for trusted interfaces within a QoS domain, use the **auto qos trust** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

auto qos trust {**cos** | **dscp** }

no auto qos trust {**cos** | **dscp**}

Syntax Description

cos	Trusts the CoS packet classification.
dscp	Trusts the DSCP packet classification.

Command Default

Auto-QoS trust is disabled on the port.

When auto-QoS is enabled, it uses the ingress packet label to categorize traffic, to assign packet labels, and to configure the ingress and egress queues. For more information, see Table 5: Traffic Types, Packet Labels, and Queues, on page 17

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS 15.0(2)EX	This command was introduced.

Usage Guidelines

Use this command to configure the QoS for trusted interfaces within the QoS domain. The QoS domain includes the switch, the network interior, and edge devices that can classify incoming traffic for QoS.

Table 5: Traffic Types, Packet Labels, and Queues

	VOIP Data Traffic	VOIP Control Traffic	Routing Protocol Traffic	STP[1] BPDU[2] Traffic	Real-Time Video Traffic	All Other Traffic	
DSCP[3]	46	24, 26	48	56	34	–	
CoS[4]	5	3	6	7	3	–	
CoS-to-egress queue map	4, 5 (queue 1)	2, 3, 6, 7 (queue 2)			0 (queue 3)	2 (queue 3)	0, 1 (queue 4)

1 STP = Spanning Tree Protocol
2 BPDU = bridge protocol data unit
3 DSCP = Differentiated Services Code Point
4 CoS = class of service

Table 6: Auto-QoS Configuration for the Egress Queues

Egress Queue	Queue Number	CoS-to-Queue Map	Queue Weight (Bandwidth)	Queue (Buffer) Size for Gigabit-Capable Ports	Queue (Buffer) Size for 10/100 Ethernet Ports
Priority (shaped)	1	4, 5	up to 100 percent	15 percent	15 percent
SRR shared	2	2, 3, 6,7	10 percent	25 percent	25 percent
SRR shared	3	0	60 percent	40 percent	40 percent
SRR shared	4	1	20 percent	20 percent	20 percent

To display the QoS configuration that is automatically generated when auto-QoS is enabled, enable debugging before you enable auto-QoS. Use the **debug auto qos** privileged EXEC command to enable auto-QoS debugging.

This is the auto-QoS generated configuration for the **auto qos trust cos** command:

```
Switch config-if)#
Mar 16 02:57:46.351 PST: mls qos map cos-dscp 0 8 16 24 32 46 48 56
Mar 16 02:57:46.351 PST: mls qos
Mar 16 02:57:46.351 PST: no mls qos srr-queue output cos-map
Mar 16 02:57:46.362 PST: no mls qos queue-set output 2 threshold
Mar 16 02:57:46.379 PST: no mls qos queue-set output 2 buffers
Mar 16 02:57:46.382 PST: mls qos srr-queue output cos-map queue 1 threshold 3  4 5
Mar 16 02:57:46.386 PST: mls qos srr-queue output cos-map queue 2 threshold 1  2
Mar 16 02:57:46.393 PST: mls qos srr-queue output cos-map queue 2 threshold 2  3
Mar 16 02:57:46.403 PST: mls qos srr-queue output cos-map queue 2 threshold 3  6 7
Mar 16 02:57:46.407 PST: mls qos srr-queue output cos-map queue 3 threshold 3  0
Mar 16 02:57:46.410 PST: mls qos srr-queue output cos-map queue 4 threshold 3  1
Mar 16 02:57:46.414 PST: no mls qos srr-queue output dscp-map
Mar 16 02:57:46.417 PST: mls qos srr-queue output dscp-map queue 1 threshold 3  32 33 40
41 42 43 44 45
Mar 16 02:57:46.417 PST: mls qos srr-queue output dscp-map queue 1 threshold 3  46 47
Mar 16 02:57:46.421 PST: mls qos srr-queue output dscp-map queue 2 threshold 1  16 17 18
19 20 21 22 23
Mar 16 02:57:46.421 PST: mls qos srr-queue output dscp-map queue 2 threshold 1  26 27 28
29 30 31 34
Mar 16 02:57:46.424 PST: mls qos srr-queue output dscp-map queue 2 threshold 1  35 36 37
38 39
Mar 16 02:57:46.428 PST: mls qos srr-queue output dscp-map queue 2 threshold 2  24
Mar 16 02:57:46.431 PST: mls qos srr-queue output dscp-map queue 2 threshold 3  48 49 50
51 52 53 54 55
Mar 16 02:57:46.442 PST: mls qos srr-queue output dscp-map queue 2 threshold 3  56 57 58
59 60 61 62 63
Mar 16 02:57:46.445 PST: mls qos srr-queue output dscp-map queue 3 threshold 3  0 1 2 3 4
5 6 7
Mar 16 02:57:46.449 PST: mls qos srr-queue output dscp-map queue 4 threshold 1  8 9 11 13
15
Mar 16 02:57:46.452 PST: mls qos srr-queue output dscp-map queue 4 threshold 2  10 12 14
Mar 16 02:57:46.456 PST: mls qos queue-set output 1 threshold 1 100 100 50 200
Mar 16 02:57:46.463 PST: mls qos queue-set output 1 threshold 2 125 125 100 400
```

```
Mar 16 02:57:46.466 PST: mls qos queue-set output 1 threshold 3 100 100 100 400
Mar 16 02:57:46.470 PST: mls qos queue-set output 1 threshold 4 60 150 50 200
Mar 16 02:57:46.473 PST: mls qos queue-set output 1 buffers 15 25 40 20
Mar 16 02:57:46.484 PST: auto qos srnd4
Mar 16 02:57:46.501 PST:   mls qos trust cos
Mar 16 02:57:46.505 PST:  no queue-set 1
Mar 16 02:57:46.505 PST:   queue-set 1
Mar 16 02:57:46.508 PST:  priority-queue out
Mar 16 02:57:46.512 PST:  srr-queue bandwidth share 1 30 35 5
```

This is the auto-QoS generated configuration for the **auto qos trust dscp** command:

```
Switch (config-if)#
switch1(config-if)#
Mar 16 02:58:40.430 PST: mls qos map cos-dscp 0 8 16 24 32 46 48 56
Mar 16 02:58:40.433 PST: mls qos
Mar 16 02:58:40.433 PST: no mls qos srr-queue output cos-map
Mar 16 02:58:40.444 PST: no mls qos queue-set output 2 threshold
Mar 16 02:58:40.458 PST: no mls qos queue-set output 2 buffers
Mar 16 02:58:40.461 PST: mls qos srr-queue output cos-map queue 1 threshold 3  4 5
Mar 16 02:58:40.465 PST: mls qos srr-queue output cos-map queue 2 threshold 1  2
Mar 16 02:58:40.468 PST: mls qos srr-queue output cos-map queue 2 threshold 2  3
Mar 16 02:58:40.472 PST: mls qos srr-queue output cos-map queue 2 threshold 3  6 7
Mar 16 02:58:40.482 PST: mls qos srr-queue output cos-map queue 3 threshold 3  0
Mar 16 02:58:40.486 PST: mls qos srr-queue output cos-map queue 4 threshold 3  1
Mar 16 02:58:40.489 PST: no mls qos srr-queue output dscp-map
Mar 16 02:58:40.496 PST: mls qos srr-queue output dscp-map queue 1 threshold 3  32 33 40
41 42 43 44 45
Mar 16 02:58:40.496 PST: mls qos srr-queue output dscp-map queue 1 threshold 3  46 47
Mar 16 02:58:40.500 PST: mls qos srr-queue output dscp-map queue 2 threshold 1  16 17 18
19 20 21 22 23
Mar 16 02:58:40.503 PST: mls qos srr-queue output dscp-map queue 2 threshold 1  26 27 28
29 30 31 34
Mar 16 02:58:40.503 PST: mls qos srr-queue output dscp-map queue 2 threshold 1  35 36 37
38 39
Mar 16 02:58:40.506 PST: mls qos srr-queue output dscp-map queue 2 threshold 2  24
Mar 16 02:58:40.510 PST: mls qos srr-queue output dscp-map queue 2 threshold 3  48 49 50
51 52 53 54 55
Mar 16 02:58:40.513 PST: mls qos srr-queue output dscp-map queue 2 threshold 3  56 57 58
59 60 61 62 63
Mar 16 02:58:40.524 PST: mls qos srr-queue output dscp-map queue 3 threshold 3  0 1 2 3 4
5 6 7
Mar 16 02:58:40.527 PST: mls qos srr-queue output dscp-map queue 4 threshold 1  8 9 11 13
15
Mar 16 02:58:40.531 PST: mls qos srr-queue output dscp-map queue 4 threshold 2  10 12 14
Mar 16 02:58:40.538 PST: mls qos queue-set output 1 threshold 1 100 100 50 200
Mar 16 02:58:40.541 PST: mls qos queue-set output 1 threshold 2 125 125 100 400
Mar 16 02:58:40.545 PST: mls qos queue-set output 1 threshold 3 100 100 100 400
Mar 16 02:58:40.548 PST: mls qos queue-set output 1 threshold 4 60 150 50 200
Mar 16 02:58:40.562 PST: mls qos queue-set output 1 buffers 15 25 40 20
Mar 16 02:58:40.566 PST: auto qos srnd4
Mar 16 02:58:40.583 PST:   mls qos trust dscp
Mar 16 02:58:40.590 PST:  no queue-set 1
Mar 16 02:58:40.590 PST:   queue-set 1
Mar 16 02:58:40.590 PST:  priority-queue out
Mar 16 02:58:40.601 PST:  srr-queue bandwidth share 1 30 35 5
```

Note The switch applies the auto-QoS-generated commands as if the commands were entered from the command-line interface (CLI). An existing user configuration can cause the application of the generated commands to fail or to be overridden by the generated commands. These actions occur without warning. If all the generated commands are successfully applied, any user-entered configuration that was not overridden remains in the running configuration. Any user-entered configuration that was overridden can be retrieved by reloading the switch without saving the current configuration to memory. If the generated commands fail to be applied, the previous running configuration is restored.

After auto-QoS is enabled, do not modify a policy map or aggregate policer that includes *AutoQoS* in its name. If you need to modify the policy map or aggregate policer, make a copy of it, and change the copied policy map or policer. To use the new policy map instead of the generated one, remove the generated policy map from the interface and apply the new policy map.

Note To disable auto-QoS, you need to remove the auto-QoS commands manually.

Enter the **no mls qos** global configuration command. With QoS disabled, there is no concept of trusted or untrusted ports because the packets are not modified (the CoS, DSCP, and IP precedence values in the packet are not changed). Traffic is switched in pass-through mode (packets are switched without any rewrites and classified as best effort without any policing).

To disable auto-QoS on a port, use the **no auto qos trust** interface configuration command. Only the auto-QoS-generated interface configuration commands for this port are removed. If this is the last port on which auto-QoS is enabled and you enter the **no auto qos trust** command, auto-QoS is considered disabled even though the auto-QoS-generated global configuration commands remain (to avoid disrupting traffic on other ports affected by the global configuration).

Examples

This example shows how to enable auto-QoS for a trusted interface with specific CoS classification:

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# auto qos trust cos
```

You can verify your settings by entering the **show auto qos interface** *interface-id* privileged EXEC command.

Related Commands

Command	Description
debug auto qos, on page 31	Enables debugging of the auto-QoS feature.
mls qos trust, on page 73	Configures the port trust state.
queue-set, on page 82	Maps a port to a queue-set.
show auto qos, on page 34	Displays auto-QoS information.
srr-queue bandwidth share, on page 104	Assigns the shared weights and enables bandwidth sharing on the four egress queues mapped to a port.
srr-queue bandwidth share, on page 104	Assigns the shared weights and enables bandwidth sharing on the four egress queues mapped to a port.

auto qos video

To automatically configure quality of service (QoS) for video within a QoS domain, use the **auto qos video** command in interface configuration mode. Use the **no** form of this command to return to the default setting.

auto qos video {**cts** | **ip-camera** | **media-player**}

no auto qos video {**cts** | **ip-camera** | **media-player**}

Syntax Description

cts	Identifies this port as connected to a Cisco TelePresence System and automatically configures QoS for video.
ip-camera	Identifies this port as connected to a Cisco IP camera and automatically configures QoS for video.
media-player	Identifies this port as connected to a CDP-capable Cisco digital media player and automatically configures QoS for video.

Command Default

Auto-QoS video is disabled on the port.

When auto-QoS is enabled, it uses the ingress packet label to categorize traffic, to assign packet labels, and to configure the ingress and egress queues.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS 15.0(2)EX	This command was introduced.

Usage Guidelines

Use this command to configure the QoS appropriate for video traffic within the QoS domain. The QoS domain includes the switch, the network interior, and edge devices that can classify incoming traffic for QoS.

Table 7: Traffic Types, Packet Labels, and Queues

	VOIP Data Traffic	VOIP Control Traffic	Routing Protocol Traffic	STP[5] BPDU[6] Traffic	Real-Time Video Traffic	All Other Traffic
DSCP[7]	46	24, 26	48	56	34	–
CoS[8]	5	3	6	7	3	–

	VOIP Data Traffic	VOIP Control Traffic	Routing Protocol Traffic	STP[5] BPDU[6] Traffic	Real-Time Video Traffic	All Other Traffic	
CoS-to-egress queue map	4, 5 (queue 1)	2, 3, 6, 7 (queue 2)	2, 3, 6, 7 (queue 2)	2, 3, 6, 7 (queue 2)	0 (queue 3)	2 (queue 3)	0, 1 (queue 4)

5 STP = Spanning Tree Protocol
6 BPDU = bridge protocol data unit
7 DSCP = Differentiated Services Code Point
8 CoS = class of service

Table 8: Auto-QoS Configuration for the Egress Queues

Egress Queue	Queue Number	CoS-to-Queue Map	Queue Weight (Bandwidth)	Queue (Buffer) Size for Gigabit-Capable Ports	Queue (Buffer) Size for 10/100 Ethernet Ports
Priority (shaped)	1	4, 5	up to 100 percent	15 percent	15 percent
SRR shared	2	2, 3, 6, 7	10 percent	25 percent	25 percent
SRR shared	3	0	60 percent	40 percent	40 percent
SRR shared	4	1	20 percent	20 percent	20 percent

Auto-QoS configures the switch for video connectivity to a Cisco TelePresence system, a Cisco IP camera, or a Cisco digital media player.

To take advantage of the auto-QoS defaults, enable auto-QoS before you configure other QoS commands. You can fine-tune the auto-QoS configuration after you enable auto-QoS.

To display the QoS configuration that is automatically generated when auto-QoS is enabled, enable debugging before you enable auto-QoS. Use the **debug auto qos** privileged EXEC command to enable auto-QoS debugging.

This is the QoS configuration that is automatically generated for the **auto qos video cts** command:

```
Switch(config-if)# auto qos video cts

Mar 16 02:54:17.286 PST: mls qos map cos-dscp 0 8 16 24 32 46 48 56
Mar 16 02:54:17.296 PST: mls qos
Mar 16 02:54:17.296 PST: no mls qos srr-queue output cos-map
Mar 16 02:54:17.300 PST: no mls qos queue-set output 2 threshold
Mar 16 02:54:17.324 PST: no mls qos queue-set output 2 buffers
Mar 16 02:54:17.328 PST: mls qos srr-queue output cos-map queue 1 threshold 3  4 5
Mar 16 02:54:17.331 PST: mls qos srr-queue output cos-map queue 2 threshold 1  2
Mar 16 02:54:17.331 PST: mls qos srr-queue output cos-map queue 2 threshold 2  3
Mar 16 02:54:17.338 PST: mls qos srr-queue output cos-map queue 2 threshold 3  6 7
Mar 16 02:54:17.338 PST: mls qos srr-queue output cos-map queue 3 threshold 3  0
Mar 16 02:54:17.342 PST: mls qos srr-queue output cos-map queue 4 threshold 3  1
Mar 16 02:54:17.345 PST: no mls qos srr-queue output dscp-map
```

```
Mar 16 02:54:17.349 PST: mls qos srr-queue output dscp-map queue 1 threshold 3  32 33 40
41 42 43 44 45
Mar 16 02:54:17.363 PST: mls qos srr-queue output dscp-map queue 1 threshold 3  46 47
Mar 16 02:54:17.366 PST: mls qos srr-queue output dscp-map queue 2 threshold 1  16 17 18
19 20 21 22 23
Mar 16 02:54:17.370 PST: mls qos srr-queue output dscp-map queue 2 threshold 1  26 27 28
29 30 31 34
Mar 16 02:54:17.373 PST: mls qos srr-queue output dscp-map queue 2 threshold 1  35 36 37
38 39
Mar 16 02:54:17.380 PST: mls qos srr-queue output dscp-map queue 2 threshold 2  24
Mar 16 02:54:17.384 PST: mls qos srr-queue output dscp-map queue 2 threshold 3  48 49 50
51 52 53 54 55
Mar 16 02:54:17.387 PST: mls qos srr-queue output dscp-map queue 2 threshold 3  56 57 58
59 60 61 62 63
Mar 16 02:54:17.391 PST: mls qos srr-queue output dscp-map queue 3 threshold 3  0 1 2 3 4
5 6 7
Mar 16 02:54:17.401 PST: mls qos srr-queue output dscp-map queue 4 threshold 1  8 9 11 13
15
Mar 16 02:54:17.405 PST: mls qos srr-queue output dscp-map queue 4 threshold 2  10 12 14
Mar 16 02:54:17.408 PST: mls qos queue-set output 1 threshold 1 100 100 50 200
Mar 16 02:54:17.415 PST: mls qos queue-set output 1 threshold 2 125 125 100 400
Mar 16 02:54:17.419 PST: mls qos queue-set output 1 threshold 3 100 100 100 400
Mar 16 02:54:17.422 PST: mls qos queue-set output 1 threshold 4 60 150 50 200
Mar 16 02:54:17.426 PST: mls qos queue-set output 1 buffers 15 25 40 20
Mar 16 02:54:17.433 PST: auto qos srnd4
Mar 16 02:54:17.454 PST:   mls qos trust device cts
Mar 16 02:54:17.457 PST:   mls qos trust dscp
Mar 16 02:54:17.464 PST:  no queue-set 1
Mar 16 02:54:17.464 PST:   queue-set 1
Mar 16 02:54:17.468 PST:  priority-queue out
Mar 16 02:54:17.482 PST:  srr-queue bandwidth share 1 30 35 5
```

This is the QoS configuration that is automatically generated for the **auto qos video ip-camera** command:

```
Switch(config-if)# auto qos video ip-camera
Mar 16 02:55:43.675 PST: mls qos map cos-dscp 0 8 16 24 32 46 48 56
Mar 16 02:55:43.685 PST: mls qos
Mar 16 02:55:43.685 PST: no mls qos srr-queue output cos-map
Mar 16 02:55:43.689 PST: no mls qos queue-set output 2 threshold
Mar 16 02:55:43.703 PST: no mls qos queue-set output 2 buffers
Mar 16 02:55:43.706 PST: mls qos srr-queue output cos-map queue 1 threshold 3  4 5
Mar 16 02:55:43.710 PST: mls qos srr-queue output cos-map queue 2 threshold 1  2
Mar 16 02:55:43.710 PST: mls qos srr-queue output cos-map queue 2 threshold 2  3
Mar 16 02:55:43.724 PST: mls qos srr-queue output cos-map queue 2 threshold 3  6 7
Mar 16 02:55:43.727 PST: mls qos srr-queue output cos-map queue 3 threshold 3  0
Mar 16 02:55:43.731 PST: mls qos srr-queue output cos-map queue 4 threshold 3  1
Mar 16 02:55:43.734 PST: no mls qos srr-queue output dscp-map
Mar 16 02:55:43.741 PST: mls qos srr-queue output dscp-map queue 1 threshold 3  32 33 40
41 42 43 44 45
Mar 16 02:55:43.745 PST: mls qos srr-queue output dscp-map queue 1 threshold 3  46 47
Mar 16 02:55:43.748 PST: mls qos srr-queue output dscp-map queue 2 threshold 1  16 17 18
19 20 21 22 23
Mar 16 02:55:43.762 PST: mls qos srr-queue output dscp-map queue 2 threshold 1  26 27 28
29 30 31 34
Mar 16 02:55:43.766 PST: mls qos srr-queue output dscp-map queue 2 threshold 1  35 36 37
38 39
Mar 16 02:55:43.769 PST: mls qos srr-queue output dscp-map queue 2 threshold 2  24
Mar 16 02:55:43.773 PST: mls qos srr-queue output dscp-map queue 2 threshold 3  48 49 50
51 52 53 54 55
Mar 16 02:55:43.780 PST: mls qos srr-queue output dscp-map queue 2 threshold 3  56 57 58
59 60 61 62 63
Mar 16 02:55:43.783 PST: mls qos srr-queue output dscp-map queue 3 threshold 3  0 1 2 3 4
5 6 7
Mar 16 02:55:43.786 PST: mls qos srr-queue output dscp-map queue 4 threshold 1  8 9 11 13
15
Mar 16 02:55:43.790 PST: mls qos srr-queue output dscp-map queue 4 threshold 2  10 12 14
Mar 16 02:55:43.793 PST: mls qos queue-set output 1 threshold 1 100 100 50 200
Mar 16 02:55:43.804 PST: mls qos queue-set output 1 threshold 2 125 125 100 400
Mar 16 02:55:43.807 PST: mls qos queue-set output 1 threshold 3 100 100 100 400
Mar 16 02:55:43.811 PST: mls qos queue-set output 1 threshold 4 60 150 50 200
Mar 16 02:55:43.814 PST: mls qos queue-set output 1 buffers 15 25 40 20
Mar 16 02:55:43.818 PST: auto qos srnd4
```

```
Mar 16 02:55:43.832 PST:   mls qos trust device ip-camera
Mar 16 02:55:43.842 PST:   mls qos trust dscp
Mar 16 02:55:43.849 PST:  no queue-set 1
Mar 16 02:55:43.849 PST:   queue-set 1
Mar 16 02:55:43.849 PST:  priority-queue out
Mar 16 02:55:43.853 PST:  srr-queue bandwidth share 1 30 35 5
```

This is the QoS configuration that is automatically generated for the **auto qos video media-player** command:

```
Switch(config-if)# auto qos video media-player
Mar 16 02:56:39.969 PST: mls qos map cos-dscp 0 8 16 24 32 46 48 56
Mar 16 02:56:39.980 PST: mls qos
Mar 16 02:56:39.980 PST: no mls qos srr-queue output cos-map
Mar 16 02:56:39.987 PST: no mls qos queue-set output 2 threshold
Mar 16 02:56:40.011 PST: no mls qos queue-set output 2 buffers
Mar 16 02:56:40.011 PST: mls qos srr-queue output cos-map queue 1 threshold 3  4 5
Mar 16 02:56:40.015 PST: mls qos srr-queue output cos-map queue 2 threshold 1  2
Mar 16 02:56:40.018 PST: mls qos srr-queue output cos-map queue 2 threshold 2  3
Mar 16 02:56:40.018 PST: mls qos srr-queue output cos-map queue 2 threshold 3  6 7
Mar 16 02:56:40.022 PST: mls qos srr-queue output cos-map queue 3 threshold 3  0
Mar 16 02:56:40.022 PST: mls qos srr-queue output cos-map queue 4 threshold 3  1
Mar 16 02:56:40.029 PST: no mls qos srr-queue output dscp-map
Mar 16 02:56:40.029 PST: mls qos srr-queue output dscp-map queue 1 threshold 3  32 33 40
41 42 43 44 45
Mar 16 02:56:40.043 PST: mls qos srr-queue output dscp-map queue 1 threshold 3  46 47
Mar 16 02:56:40.046 PST: mls qos srr-queue output dscp-map queue 2 threshold 1  16 17 18
19 20 21 22 23
Mar 16 02:56:40.050 PST: mls qos srr-queue output dscp-map queue 2 threshold 1  26 27 28
29 30 31 34
Mar 16 02:56:40.053 PST: mls qos srr-queue output dscp-map queue 2 threshold 1  35 36 37
38 39
Mar 16 02:56:40.057 PST: mls qos srr-queue output dscp-map queue 2 threshold 2  24
Mar 16 02:56:40.064 PST: mls qos srr-queue output dscp-map queue 2 threshold 3  48 49 50
51 52 53 54 55
Mar 16 02:56:40.067 PST: mls qos srr-queue output dscp-map queue 2 threshold 3  56 57 58
59 60 61 62 63
Mar 16 02:56:40.071 PST: mls qos srr-queue output dscp-map queue 3 threshold 3  0 1 2 3 4
5 6 7
Mar 16 02:56:40.081 PST: mls qos srr-queue output dscp-map queue 4 threshold 1  8 9 11 13
15
Mar 16 02:56:40.085 PST: mls qos srr-queue output dscp-map queue 4 threshold 2  10 12 14
Mar 16 02:56:40.092 PST: mls qos queue-set output 1 threshold 1 100 100 50 200
Mar 16 02:56:40.095 PST: mls qos queue-set output 1 threshold 2 125 125 100 400
Mar 16 02:56:40.099 PST: mls qos queue-set output 1 threshold 3 100 100 100 400
Mar 16 02:56:40.102 PST: mls qos queue-set output 1 threshold 4 60 150 50 200
Mar 16 02:56:40.106 PST: mls qos queue-set output 1 buffers 15 25 40 20
Mar 16 02:56:40.109 PST: auto qos srnd4
Mar 16 02:56:40.130 PST:   mls qos trust device media-player
Mar 16 02:56:40.133 PST:   mls qos trust dscp
Mar 16 02:56:40.137 PST:  no queue-set 1
Mar 16 02:56:40.137 PST:   queue-set 1
Mar 16 02:56:40.140 PST:  priority-queue out
Mar 16 02:56:40.172 PST:  srr-queue bandwidth share 1 30 35 5
```

Note The switch applies the auto-QoS-generated commands as if the commands were entered from the command-line interface (CLI). An existing user configuration can cause the application of the generated commands to fail or to be overridden by the generated commands. These actions occur without warning. If all the generated commands are successfully applied, any user-entered configuration that was not overridden remains in the running configuration. Any user-entered configuration that was overridden can be retrieved by reloading the switch without saving the current configuration to memory. If the generated commands fail to be applied, the previous running configuration is restored.

If this is the first port on which you have enabled auto-QoS, the auto-QoS-generated global configuration commands are executed followed by the interface configuration commands. If you enable auto-QoS on another port, only the auto-QoS-generated interface configuration commands for that port are executed.

When you enable the auto-QoS feature on the first port, QoS is globally enabled (**mls qos** global configuration command), and other global configuration commands are added.

After auto-QoS is enabled, do not modify a policy map or aggregate policer that includes *AutoQoS* in its name. If you need to modify the policy map or aggregate policer, make a copy of it, and change the copied policy map or policer. To use the new policy map instead of the generated one, remove the generated policy map from the interface, and apply the new policy map.

Note To disable auto-QoS, you need to remove the auto-QoS commands manually.

Enter the **no mls qos** global configuration command to disable the auto-QoS-generated global configuration commands. With QoS disabled, there is no concept of trusted or untrusted ports because the packets are not modified (the CoS, DSCP, and IP precedence values in the packet are not changed). Traffic is switched in pass-through mode (packets are switched without any rewrites and classified as best effort without any policing).

To disable auto-QoS on a port, use the **no auto qos video** interface configuration command. Only the auto-QoS-generated interface configuration commands for this port are removed. If this is the last port on which auto-QoS is enabled and you enter the **no auto qos video** command, auto-QoS is considered disabled even though the auto-QoS-generated global configuration commands remain (to avoid disrupting traffic on other ports affected by the global configuration).

Examples

This example shows how to enable auto-QoS for a Cisco Telepresence interface with conditional trust. The interface is trusted only if a Cisco Telepresence device is detected; otherwise, the port is untrusted.

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# auto qos video cts
```

You can verify your settings by entering the **show auto qos video interface** *interface-id* privileged EXEC command.

Related Commands

Command	Description
debug auto qos, on page 31	Enables debugging of the auto-QoS feature.
mls qos trust, on page 73	Configures the port trust state.
queue-set, on page 82	Maps a port to a queue-set.
show auto qos, on page 34	Displays auto-QoS information.
show mls qos interface, on page 91	Displays QoS information at the port level.
srr-queue bandwidth share, on page 104	Assigns the shared weights and enables bandwidth sharing on the four egress queues mapped to a port.

auto qos voip

To automatically configure quality of service (QoS) for voice over IP (VoIP) within a QoS domain, use the **auto qos voip** command in interface configuration mode. Use the **no** form of this command to return to the default setting.

auto qos voip {**cisco-phone** | **cisco-softphone** | **trust**}

no auto qos voip {**cisco-phone** | **cisco-softphone** | **trust**}

Syntax Description

cisco-phone	Identifies this port as connected to a Cisco IP Phone, and automatically configures QoS for VoIP. The QoS labels of incoming packets are trusted only when the telephone is detected.
cisco-softphone	Identifies this port as connected to a device running the Cisco SoftPhone, and automatically configures QoS for VoIP.
trust	Identifies this port as connected to a trusted switch, and automatically configures QoS for VoIP. The QoS labels of incoming packets are trusted. For nonrouted ports, the CoS value of the incoming packet is trusted. For routed ports, the DSCP value of the incoming packet is trusted.

Command Default

Auto-QoS is disabled on the port.

When auto-QoS is enabled, it uses the ingress packet label to categorize traffic, assign packet labels, and configure the ingress and egress queues. For more information, seeTable 9: Traffic Types, Packet Labels, and Queues, on page 27

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS 15.0(2)EX	This command was introduced.

Usage Guidelines

Use this command to configure the QoS appropriate for VoIP traffic within the QoS domain. The QoS domain includes the switch, the network interior, and edge devices that can classify incoming traffic for QoS.

Auto-QoS configures the switch for VoIP with Cisco IP Phones on switch and routed ports and for VoIP with devices running the Cisco SoftPhone application. These releases support only Cisco IP SoftPhone Version 1.3(3) or later. Connected devices must use Cisco Call Manager Version 4 or later.

To take advantage of the auto-QoS defaults, enable auto-QoS before you configure other QoS commands. You can fine-tune the auto-QoS configuration after you enable auto-QoS.

Table 9: Traffic Types, Packet Labels, and Queues

	VOIP Data Traffic	VOIP Control Traffic	Routing Protocol Traffic	STP[9] BPDU[10] Traffic	Real-Time Video Traffic	All Other Traffic	
DSCP[11]	46	24, 26	48	56	34	–	
CoS[12]	5	3	6	7	3	–	
CoS-to-egress queue map	4, 5 (queue 1)	2, 3, 6, 7 (queue 2)	2, 3, 6, 7 (queue 2)	2, 3, 6, 7 (queue 2)	0 (queue 3)	2 (queue 3)	0, 1 (queue 4)

9 STP = Spanning Tree Protocol
10 BPDU = bridge protocol data unit
11 DSCP = Differentiated Services Code Point
12 CoS = class of service

The switch configures egress queues on the port according to the settings in this table.

Table 10: Auto-QoS Configuration for the Egress Queues

Egress Queue	Queue Number	CoS-to-Queue Map	Queue Weight (Bandwidth)	Queue (Buffer) Size for Gigabit-Capable Ports	Queue (Buffer) Size for 10/100 Ethernet Ports
Priority (shaped)	1	4, 5	up to 100 percent	15 percent	15 percent
SRR shared	2	2, 3, 6, 7	10 percent	25 percent	25 percent
SRR shared	3	0	60 percent	40 percent	40 percent
SRR shared	4	1	20 percent	20 percent	20 percent

Note The switch applies the auto-QoS-generated commands as if the commands were entered from the command-line interface (CLI). An existing user configuration can cause the application of the generated commands to fail or to be overridden by the generated commands. These actions occur without warning. If all the generated commands are successfully applied, any user-entered configuration that was not overridden remains in the running configuration. Any user-entered configuration that was overridden can be retrieved by reloading the switch without saving the current configuration to memory. If the generated commands fail to be applied, the previous running configuration is restored.

If this is the first port on which you have enabled auto-QoS, the auto-QoS-generated global configuration commands are executed followed by the interface configuration commands. If you enable auto-QoS on another port, only the auto-QoS-generated interface configuration commands for that port are executed.

When you enable the auto-QoS feature on the first port, these automatic actions occur:

- QoS is globally enabled (**mls qos** global configuration command), and other global configuration commands are added.
- When you enter the **auto qos voip cisco-phone** interface configuration command on a port at the edge of the network that is connected to a Cisco IP Phone, the switch enables the trusted boundary feature. The switch uses the Cisco Discovery Protocol (CDP) to detect the presence of a Cisco IP Phone. When a Cisco IP Phone is detected, the ingress classification on the port is set to trust the QoS label received in the packet. The switch also uses policing to determine whether a packet is in or out of profile and to specify the action on the packet. If the packet does not have a DSCP value of 24, 26, or 46 or is out of profile, the switch changes the DSCP value to 0. When a Cisco IP Phone is absent, the ingress classification is set to not trust the QoS label in the packet. The policing is applied to the traffic that matches the policy-map classification before the switch enables the trust boundary feature.
- When you enter the **auto qos voip cisco-softphone** interface configuration command on a port at the edge of the network that is connected to a device running the Cisco SoftPhone, the switch uses policing to decide whether a packet is in or out of profile and to specify the action on the packet. If the packet does not have a DSCP value of 24, 26, or 46 or is out of profile, the switch changes the DSCP value to 0.
- When you enter the **auto qos voip trust** interface configuration command on a port connected to the network interior, the switch trusts the CoS value for nonrouted ports or the DSCP value for routed ports in ingress packets (the assumption is that traffic has already been classified by other edge devices).

You can enable auto-QoS on static, dynamic-access, and voice VLAN access, and trunk ports. When enabling auto-QoS with a Cisco IP Phone on a routed port, you must assign a static IP address to the IP phone.

Note When a device running Cisco SoftPhone is connected to a switch or routed port, the switch supports only one Cisco SoftPhone application per port.

After auto-QoS is enabled, do not modify a policy map or aggregate policer that includes *AutoQoS* in its name. If you need to modify the policy map or aggregate policer, make a copy of it, and change the copied policy map or policer. To use the new policy map instead of the generated one, remove the generated policy map from the interface, and apply the new policy map.

To display the QoS configuration that is automatically generated when auto-QoS is enabled, enable debugging before you enable auto-QoS. Use the **debug auto qos** privileged EXEC command to enable auto-QoS debugging.

Note To disable auto-QoS, you need to remove the auto-QoS commands manually.

Enter the **no mls qos** global configuration command to disable the auto-QoS-generated global configuration commands. With QoS disabled, there is no concept of trusted or untrusted ports because the packets are not modified (the CoS, DSCP, and IP precedence values in the packet are not changed). Traffic is switched in pass-through mode. Packets are switched without any rewrites and classified as best effort without any policing.

To disable auto-QoS on a port, use the **no auto qos voip** interface configuration command. Only the auto-QoS-generated interface configuration commands for this port are removed. If this is the last port on

which auto-QoS is enabled and you enter the **no auto qos voip** command, auto-QoS is considered disabled even though the auto-QoS-generated global configuration commands remain (to avoid disrupting traffic on other ports affected by the global configuration).

This is the enhanced configuration for the **auto qos voip cisco-phone** command:

```
Switch(config)# mls qos map policed-dscp  0 10 18 to 8
Switch(config)# mls qos map cos-dscp 0 8 16 24 32 46 48 56
Switch(config)# class-map match-all AUTOQOS_VOIP_DATA_CLASS
Switch(config-cmap)# match ip dscp ef
Switch(config)# class-map match-all AUTOQOS_DEFAULT_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-DEFAULT
Switch(config)# class-map match-all AUTOQOS_VOIP_SIGNAL_CLASS
Switch(config-cmap)# match ip dscp cs3
Switch(config)# policy-map AUTOQOS-SRND4-CISCOPHONE-POLICY
Switch(config-pmap)# class AUTOQOS_VOIP_DATA_CLASS
Switch(config-pmap-c)# set dscp ef
Switch(config-pmap-c)# police 128000 8000 exceed-action policed-dscp-transmit
Switch(config-pmap)# class AUTOQOS_VOIP_SIGNAL_CLASS
Switch(config-pmap-c)# set dscp cs3
Switch(config-pmap-c)# police 32000 8000 exceed-action policed-dscp-transmit
Switch(config-pmap)# class AUTOQOS_DEFAULT_CLASS
Switch(config-pmap-c)# set dscp default
Switch(config-pmap-c)# police 10000000 8000 exceed-action policed-dscp-transmit
Switch(config-if)# service-policy input AUTOQOS-SRND4-CISCOPHONE-POLICY
```

This is the enhanced configuration for the **auto qos voip cisco-softphone** command:

```
Switch(config)# mls qos map policed-dscp  0 10 18 to 8
Switch(config)# mls qos map cos-dscp 0 8 16 24 32 46 48 56
Switch(config)# class-map match-all AUTOQOS_MULTIENHANCED_CONF_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-MULTIENHANCED-CONF
Switch(config)# class-map match-all AUTOQOS_VOIP_DATA_CLASS
Switch(config-cmap)# match ip dscp ef
Switch(config)# class-map match-all AUTOQOS_DEFAULT_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-DEFAULT
Switch(config)# class-map match-all AUTOQOS_TRANSACTION_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-TRANSACTIONAL-DATA
Switch(config)# class-map match-all AUTOQOS_VOIP_SIGNAL_CLASS
Switch(config-cmap)# match ip dscp cs3
Switch(config)# class-map match-all AUTOQOS_SIGNALING_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-SIGNALING
Switch(config)# class-map match-all AUTOQOS_BULK_DATA_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-BULK-DATA
Switch(config)# class-map match-all AUTOQOS_SCAVANGER_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-SCAVANGER
Switch(config)# policy-map AUTOQOS-SRND4-SOFTPHONE-POLICY
Switch(config-pmap)# class AUTOQOS_VOIP_DATA_CLASS
Switch(config-pmap-c)# set dscp ef
Switch(config-pmap-c)# police 128000 8000 exceed-action policed-dscp-transmit
Switch(config-pmap)# class AUTOQOS_VOIP_SIGNAL_CLASS
Switch(config-pmap-c)# set dscp cs3
Switch(config-pmap-c)# police 32000 8000 exceed-action policed-dscp-transmit
Switch(config-pmap)# class AUTOQOS_MULTIENHANCED_CONF_CLASS
Switch(config-pmap-c)# set dscp af41
Switch(config-pmap-c)# police 5000000 8000 exceed-action drop
Switch(config-pmap)# class AUTOQOS_BULK_DATA_CLASS
Switch(config-pmap-c)# set dscp af11
Switch(config-pmap-c)# police 10000000 8000 exceed-action policed-dscp-transmit
Switch(config-pmap)# class AUTOQOS_TRANSACTION_CLASS
Switch(config-pmap-c)# set dscp af21
Switch(config-pmap-c)# police 10000000 8000 exceed-action policed-dscp-transmit
Switch(config-pmap)# class AUTOQOS_SCAVANGER_CLASS
Switch(config-pmap-c)# set dscp cs1
Switch(config-pmap-c)# police 10000000 8000 exceed-action drop
Switch(config-pmap)# class AUTOQOS_SIGNALING_CLASS
Switch(config-pmap-c)# set dscp cs3
Switch(config-pmap-c)# police 32000 8000 exceed-action drop
```

```
Switch(config-pmap)# class AUTOQOS_DEFAULT_CLASS
Switch(config-pmap-c)# set dscp default
Switch(config-if)# service-policy input AUTOQOS-SRND4-SOFTPHONE-POLICY
```

Examples

This example shows how to enable auto-QoS and to trust the QoS labels received in incoming packets when the switch or router connected to the port is a trusted device:

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# auto qos voip trust
```

You can verify your settings by entering the **show auto qos interface** *interface-id* privileged EXEC command.

Related Commands

Command	Description
debug auto qos, on page 31	Enables debugging of the auto-QoS feature.
mls qos cos, on page 54	Defines the default CoS value of a port or assigns the default CoS to all incoming packets on the port.
mls qos map, on page 58	Defines the CoS-to-DSCP map or the DSCP-to-CoS map.
mls qos queue-set output buffers, on page 62	Allocates buffers to a queue-set.
mls qos srr-queue output cos-map, on page 69	Maps CoS values to an egress queue or maps CoS values to a queue and to a threshold ID.
mls qos srr-queue output dscp-map, on page 71	Maps DSCP values to an egress queue or maps DSCP values to a queue and to a threshold ID.
mls qos trust, on page 73	Configures the port trust state.
queue-set, on page 82	Maps a port to a queue-set.
show auto qos, on page 34	Displays auto-QoS information.
show mls qos interface, on page 91	Displays QoS information at the port level.
srr-queue bandwidth shape, on page 102	Assigns the shaped weights and enables bandwidth shaping on the four egress queues mapped to a port.
srr-queue bandwidth share, on page 104	Assigns the shared weights and enables bandwidth sharing on the four egress queues mapped to a port.

debug auto qos

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

debug auto qos

no debug auto qos

Syntax Description

This command has no arguments or keywords.

Command Default

Auto-QoS debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS 15.0(2)EX	This command was introduced.

Usage Guidelines

To display the QoS configuration that is automatically generated when auto-QoS is enabled, enable debugging before you enable auto-QoS. You enable debugging by entering the **debug auto qos** privileged EXEC command.

The **undebug auto qos** command is the same as the **no debug auto qos** 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* 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 active switch to enable debugging on a member switch without first starting a session.

Examples

This example shows how to display the QoS configuration that is automatically generated when auto-QoS is enabled:

```
Switch# debug auto qos
Auto QoS debugging is on

Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)#auto qos voip cisco-softphone
May 31 09:03:32.293: no policy-map AUTOQOS-SRND4-SOFTPHONE-POLICY
May 31 09:03:32.296: %PARSE_RC-4-PRC_NON_COMPLIANCE: `no policy-map
AUTOQOS-SRND4-SOFTPHONE-POLICY '
May 31 09:03:32.296: no policy-map AUTOQOS-SRND4-CISCOPHONE-POLICY
May 31 09:03:32.300: %PARSE_RC-4-PRC_NON_COMPLIANCE: `no policy-map
AUTOQOS-SRND4-CISCOPHONE-POLICY '
May 31 09:03:32.300: no policy-map AUTOQOS-SRND4-CLASSIFY-POLICY
May 31 09:03:32.300: %PARSE_RC-4-PRC_NON_COMPLIANCE: `no policy-map
```

```
AUTOQOS-SRND4-CLASSIFY-POLICY '
May 31 09:03:32.303: %PARSE_RC-4-PRC_NON_COMPLIANCE: `no policy-map
AUTOQOS-SRND4-CLASSIFY-POLICE-POLICY '
May 31 09:03:32.303: no  class-map match-all AUTOQOS_DEFAULT_CLASS
May 31 09:03:32.307: no  class-map match-all AUTOQOS_MULTIENHANCED_CONF_CLASS
May 31 09:03:32.310: no  class-map match-all AUTOQOS_TRANSACTION_CLASS
May 31 09:03:32.310: no  class-map match-all AUTOQOS_BULK_DATA_CLASS
May 31 09:03:32.314: no  class-map match-all AUTOQOS_SCAVANGER_CLASS
May 31 09:03:32.317: no  class-map match-all AUTOQOS_SIGNALING_CLASS
May 31 09:03:32.321: no  class-map match-all AUTOQOS_VOIP_DATA_CLASS
May 31 09:03:32.324: no  class-map match-all AUTOQOS_VOIP_SIGNAL_CLASS
May 31 09:03:32.324: no  ip access-list extended AUTOQOS-ACL-DEFAULT
May 31 09:03:32.328: no  ip access-list extended AUTOQOS-ACL-BULK-DATA
May 31 09:03:32.331: no  ip access-list extended AUTOQOS-ACL-SCAVANGER
May 31 09:03:32.335: no  ip access-list extended AUTOQOS-ACL-TRANSACTIONAL-DATA
May 31 09:03:32.338: no  ip access-list extended AUTOQOS-ACL-SIGNALING
May 31 09:03:32.415: no  ip access-list extended AUTOQOS-ACL-MULTIENHANCED-CONF
May 31 09:03:32.419: mls qos map cos-dscp 0 8 16 24 32 46 48 56
May 31 09:03:32.426: mls qos
May 31 09:03:32.426: no mls qos srr-queue output cos-map
May 31 09:03:32.429: no mls qos map policed-dscp
May 31 09:03:32.446: mls qos srr-queue output cos-map queue 1 threshold 3  5
May 31 09:03:32.450: mls qos srr-queue output cos-map queue 2 threshold 3  3 6 7
May 31 09:03:32.527: mls qos srr-queue output cos-map queue 3 threshold 3  2 4
May 31 09:03:32.530: mls qos srr-queue output cos-map queue 4 threshold 2  1
May 31 09:03:32.530: mls qos srr-queue output cos-map queue 4 threshold 3  0
May 31 09:03:32.537: no mls qos srr-queue output dscp-map
May 31 09:03:32.541: mls qos srr-queue output dscp-map queue 1 threshold 3  40 41 42 43 44
 45 46 47
May 31 09:03:32.544: mls qos srr-queue output dscp-map queue 2 threshold 3  24 25 26 27 28
 29 30 31
May 31 09:03:32.544: mls qos srr-queue output dscp-map queue 2 threshold 3  48 49 50 51 52
 53 54 55
May 31 09:03:32.544: mls qos srr-queue output dscp-map queue 2 threshold 3  56 57 58 59 60
 61 62 63
May 31 09:03:32.548: mls qos srr-queue output dscp-map queue 3 threshold 3  16 17 18 19 20
 21 22 23
May 31 09:03:32.548: mls qos srr-queue output dscp-map queue 3 threshold 3  32 33 34 35 36
 37 38 39
May 31 09:03:32.621: mls qos srr-queue output dscp-map queue 4 threshold 1  8
May 31 09:03:32.628: mls qos srr-queue output dscp-map queue 4 threshold 2  9 10 11 12 13
14 15
May 31 09:03:32.751: mls qos srr-queue output dscp-map queue 4 threshold 3  0 1 2 3 4 5 6
7
May 31 09:03:32.761: mls qos queue-set output 1 threshold 1 138 138 92 138
May 31 09:03:32.779: mls qos queue-set output 1 threshold 2 138 138 92 400
May 31 09:03:32.779: mls qos queue-set output 1 threshold 3 36 77 100 318
May 31 09:03:32.782: mls qos queue-set output 1 threshold 4 20 50 67 400
May 31 09:03:32.859: mls qos queue-set output 1 buffers 10 10 26 54
May 31 09:03:33.488: no policy-map AUTOQOS-SRND4-SOFTPHONE-POLICY
May 31 09:03:33.492: %PARSE_RC-4-PRC_NON_COMPLIANCE: `no policy-map
AUTOQOS-SRND4-SOFTPHONE-POLICY '
May 31 09:03:33.492: no policy-map AUTOQOS-SRND4-CISCOPHONE-POLICY
May 31 09:03:33.495: %PARSE_RC-4-PRC_NON_COMPLIANCE: `no policy-map
AUTOQOS-SRND4-CISCOPHONE-POLICY '
May 31 09:03:33.495: no policy-map AUTOQOS-SRND4-CLASSIFY-POLICY
May 31 09:03:33.495: %PARSE_RC-4-PRC_NON_COMPLIANCE: `no policy-map
AUTOQOS-SRND4-CLASSIFY-POLICY '
May 31 09:03:33.495: no policy-map AUTOQOS-SRND4-CLASSIFY-POLICE-POLICY
May 31 09:03:33.499: %PARSE_RC-4-PRC_NON_COMPLIANCE: `no policy-map
AUTOQOS-SRND4-CLASSIFY-POLICE-POLICY '
May 31 09:03:33.499: no  class-map match-all AUTOQOS_DEFAULT_CLASS
May 31 09:03:33.499: no  class-map match-all AUTOQOS_MULTIENHANCED_CONF_CLASS
May 31 09:03:33.499: no  class-map match-all AUTOQOS_TRANSACTION_CLASS
May 31 09:03:33.502: no  class-map match-all AUTOQOS_BULK_DATA_CLASS
May 31 09:03:33.502: no  class-map match-all AUTOQOS_SCAVANGER_CLASS
May 31 09:03:33.502: no  class-map match-all AUTOQOS_SIGNALING_CLASS
May 31 09:03:33.502: no  class-map match-all AUTOQOS_VOIP_DATA_CLASS
May 31 09:03:33.502: no  class-map match-all AUTOQOS_VOIP_SIGNAL_CLASS
May 31 09:03:33.502: no  ip access-list extended AUTOQOS-ACL-DEFAULT
May 31 09:03:33.506: no  ip access-list extended AUTOQOS-ACL-BULK-DATA
May 31 09:03:33.509: no  ip access-list extended AUTOQOS-ACL-SCAVANGER
May 31 09:03:33.513: no  ip access-list extended AUTOQOS-ACL-TRANSACTIONAL-DATA
```

```
May 31 09:03:33.516: no  ip access-list extended AUTOQOS-ACL-SIGNALING
May 31 09:03:33.520: no  ip access-list extended AUTOQOS-ACL-MULTIENHANCED-CONF
May 31 09:03:33.523: no mls qos map cos-dscp
May 31 09:03:33.544: no mls qos
May 31 09:03:33.638: no mls qos srr-queue output cos-map
May 31 09:03:33.642: no mls qos map policed-dscp
May 31 09:03:33.642: no mls qos srr-queue output dscp-map
May 31 09:03:33.656: no mls qos queue-set output 1 threshold 1
May 31 09:03:33.659: no mls qos queue-set output 1 threshold 2
May 31 09:03:33.663: no mls qos queue-set output 1 threshold 3
May 31 09:03:33.663: no mls qos queue-set output 1 threshold 4
May 31 09:03:33.663: no mls qos queue-set output 1 buffers
May 31 09:03:33.782: no mls qos queue-set output 2 threshold 1
May 31 09:03:33.785: no mls qos queue-set output 2 threshold 2
May 31 09:03:33.785: no mls qos queue-set output 2 threshold 3
May 31 09:03:33.785: no mls qos queue-set output 2 threshold 4
May 31 09:03:33.789: no mls qos queue-set output 2 buffers
May 31 09:03:33.789: mls qos srr-queue output queues 8
May 31 09:03:33.792: mls qos
```

Related Commands

Command	Description
show auto qos, on page 34	Displays the initial configuration that is generated by the auto-QoS feature.
show debugging	Displays information about the types of debugging that are enabled.

show auto qos

To display the quality of service (QoS) commands entered on the interfaces on which auto-QoS is enabled, use the **show auto qos** command in privileged EXEC mode.

show auto qos [**interface** [*interface-id*]]

Syntax Description

interface [*interface-id*]	(Optional) Displays auto-QoS information for the specified port or for all ports. Valid interfaces include physical ports.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS 15.0(2)EX	This command was introduced.

Usage Guidelines

The **show auto qos** command output shows only the **auto qos** command entered on each interface. The **show auto qos interface** *interface-id* command output shows the **auto qos** command entered on a specific interface.

Use the **show running-config** privileged EXEC command to display the auto-QoS configuration and the user modifications.

The **show auto qos** command output shows the service policy information for the Cisco IP phone.

To display information about the QoS configuration that might be affected by auto-QoS, use one of these commands:

- **show mls qos**
- **show mls qos maps cos-dscp**
- **show mls qos interface** [*interface-id*] [**buffers** | **queueing**]
- **show mls qos maps** [**cos-dscp** | **cos-input-q** | **cos-output-q** | **dscp-cos** | **dscp-input-q** | **dscp-output-q**]
- **show mls qos input-queue**
- **show running-config**

Examples

This is an example of output from the **show auto qos** command after the **auto qos voip cisco-phone** and the **auto qos voip cisco-softphone** interface configuration commands are entered:

```
Switch# show auto qos
GigabitEthernet2/0/4
auto qos voip cisco-softphone
```

```
GigabitEthernet2/0/5
auto qos voip cisco-phone


GigabitEthernet2/0/6
auto qos voip cisco-phone
```

This is an example of output from the **show auto qos interface** *interface-id* command when the **auto qos voip cisco-phone** interface configuration command is entered:

```
Switch# show auto qos interface gigabitethernet 2/0/5
GigabitEthernet2/0/5
auto qos voip cisco-phone
```

This is an example of output from the **show running-config** privileged EXEC command when the **auto qos voip cisco-phone** and the **auto qos voip cisco-softphone** interface configuration commands are entered:

```
Switch# show running-config
Building configuration...
...
mls qos map policed-dscp  0 10 18 24 46 to 8
mls qos map cos-dscp 0 8 16 24 32 46 48 56
mls qos srr-queue output cos-map queue 1 threshold 3 4 5
mls qos srr-queue output cos-map queue 2 threshold 1 2
mls qos srr-queue output cos-map queue 2 threshold 2 3
mls qos srr-queue output cos-map queue 2 threshold 3 6 7
mls qos srr-queue output cos-map queue 3 threshold 3 0
mls qos srr-queue output cos-map queue 4 threshold 3 1
mls qos srr-queue output dscp-map queue 1 threshold 3 32 33 40 41 42 43 44 45
mls qos srr-queue output dscp-map queue 1 threshold 3 46 47
mls qos srr-queue output dscp-map queue 2 threshold 1 16 17 18 19 20 21 22 23
mls qos srr-queue output dscp-map queue 2 threshold 1 26 27 28 29 30 31 34 35
mls qos srr-queue output dscp-map queue 2 threshold 1 36 37 38 39
mls qos srr-queue output dscp-map queue 2 threshold 2 24
mls qos srr-queue output dscp-map queue 2 threshold 3 48 49 50 51 52 53 54 55
mls qos srr-queue output dscp-map queue 2 threshold 3 56 57 58 59 60 61 62 63
mls qos srr-queue output dscp-map queue 3 threshold 3 0 1 2 3 4 5 6 7
mls qos srr-queue output dscp-map queue 4 threshold 1 8 9 11 13 15
mls qos srr-queue output dscp-map queue 4 threshold 2 10 12 14
mls qos queue-set output 1 threshold 1 100 100 50 200
mls qos queue-set output 1 threshold 2 125 125 100 400
mls qos queue-set output 1 threshold 3 100 100 100 400
mls qos queue-set output 1 threshold 4 60 150 50 200
mls qos queue-set output 1 buffers 15 25 40 20
mls qos
...
!
spanning-tree mode pvst
spanning-tree extend system-id
!
network-policy profile 1
!
vlan access-map vmap4 10
 action forward
!
vlan internal allocation policy ascending
!
class-map match-all paul
class-map match-all cm-1
  match ip dscp af11
class-map match-all AUTOQOS_VOIP_DATA_CLASS
  match ip dscp ef
class-map match-all AUTOQOS_DEFAULT_CLASS
  match access-group name AUTOQOS-ACL-DEFAULT
class-map match-all AUTOQOS_VOIP_SIGNAL_CLASS
  match ip dscp cs3
class-map match-all ftp_class
!
policy-map AUTOQOS-SRND4-CISCOPHONE-POLICY
```

```
 class AUTOQOS_VOIP_DATA_CLASS
   set dscp ef
  police 128000 8000 exceed-action policed-dscp-transmit
 class AUTOQOS_VOIP_SIGNAL_CLASS
   set dscp cs3
  police 32000 8000 exceed-action policed-dscp-transmit
 class AUTOQOS_DEFAULT_CLASS
   set dscp default
  police 10000000 8000 exceed-action policed-dscp-transmit
policy-map policy_ftp
 class ftp_class
!!
interface FastEthernet0
 no ip address
!
interface GigabitEthernet1/0/1
 srr-queue bandwidth share 1 30 35 5
 priority-queue out
 mls qos trust cos
 auto qos trust
!
interface GigabitEthernet1/0/2
 srr-queue bandwidth share 1 30 35 5
 priority-queue out
 mls qos trust device cisco-phone
 mls qos trust cos
 auto qos voip cisco-phone
 service-policy input AUTOQOS-SRND4-CISCOPHONE-POLICY
!

<output truncated>
```

These are examples of output from the **show auto qos interface** command:

```
Switch# show auto qos interface

!
interface GigabitEthernet2/0/4
 switchport mode access
 switchport port-security maximum 400
 service-policy input AutoQoS-Police-SoftPhone
 speed 100
 duplex half
 srr-queue bandwidth share 10 10 60 20
 priority-queue out
 auto qos voip cisco-softphone
!
interface GigabitEthernet2/0/5
 switchport mode access
 switchport port-security maximum 1999
 speed 100
 duplex full
 srr-queue bandwidth share 10 10 60 20
 priority-queue out
 mls qos trust device cisco-phone
 mls qos trust cos
 auto qos voip cisco-phone
!
interface GigabitEthernet2/0/6
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 2
 switchport mode access
 speed 10
 srr-queue bandwidth share 10 10 60 20
 priority-queue out
 mls qos trust device cisco-phone
 mls qos trust cos
 auto qos voip cisco-phone
!
interface GigabitEthernet4/0/1
 srr-queue bandwidth share 10 10 60 20
 priority-queue out
```

```
 mls qos trust device cisco-phone
 mls qos trust cos
 mls qos trust device cisco-phone
service-policy input AutoQoS-Police-CiscoPhone
```

These are examples of output from the **show auto qos interface** *interface-id* command when auto-QoS is disabled on an interface:

```
Switch# show auto qos interface gigabitethernet3/0/1
AutoQoS is disabled
```

Related Commands

Command	Description
debug auto qos, on page 31	Enables debugging of the auto-QoS feature.

QoS Commands

This chapter contains the following QoS commands:

class

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

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

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

Syntax Description

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

Command Default

No policy map class-maps are defined.

Command Modes

Policy-map configuration

Command History

Release	Modification
Cisco IOS 15.0(2)EX	This command was introduced.

Usage Guidelines

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

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

- **exit—**Exits policy-map class configuration mode and returns to policy-map configuration mode.
- **no—**Returns a command to its default setting.
- **police—**Defines a policer or aggregate policer for the classified traffic. The policer specifies the bandwidth limitations and the action to take when the limits are exceeded. For more information, see police, on page 76 and police aggregate, on page 78.
- **set—**Specifies a value to be assigned to the classified traffic. For more information, see set, on page 86.
- **trust—**Defines a trust state for traffic classified with the **class** or the **class-map** command. For more information, see trust, on page 106.

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

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

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

Examples

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

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

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

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

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

Related Commands

Command	Description
class-map, on page 44	Creates a class map to be used for matching packets to the class whose name you specify.
police, on page 76	Defines a policer for classified traffic.
policy map, on page 80	Defines a policer for classified traffic.

Command	Description
set, on page 86	Classifies IP traffic by setting a DSCP or IP-precedence value in the packet.
show policy-map, on page 99	Displays quality of service (QoS) policy maps.
trust, on page 106	Defines a trust state for the traffic classified through the **class** policy-map configuration command or the **class-map** global configuration command.

class-map

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

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

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

Syntax Description

match-any	(Optional) Performs 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	Name of the class for the class map. The class name is used for both the class map and to configure a policy for the class in the policy map.

Command Default

No class maps are defined.

Command Modes

Global configuration

Policy map configuration

Command History

Release	Modification
Cisco IOS 15.0(2)EX	This command was introduced.

Usage Guidelines

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) .
- **no—**Removes a match statement from a class map.

If you enter the **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.

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*:

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

This example shows how to delete the class map *class1*:

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

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

Related Commands

Command	Description
class, on page 41	Defines a traffic classification match criteria (through the **police**, **set**, and **trust** policy-map class configuration commands) for the specified class-map name.
match (class-map configuration), on page 48	Defines the match criteria to classify traffic.
policy map, on page 80	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
show class-map, on page 88	Displays QoS class maps.

debug qos

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

debug qos {**capability**| **command-installation-time**| **events**| **index**| **pre-classify**| **provision**| **service-policy**| **set**| **snmp**| **tunnel_marking**}

no debug qos {**capability**| **command-installation-time**| **events**| **index**| **pre-classify**| **provision**| **service-policy**| **set**| **snmp**| **tunnel_marking**}

Syntax Description

capability	Displays all QoS capability debug messages.
command-installation-time	Displays the amount of time the QoS command takes to become effective.
events	Displays QoS MQC events.
index	Displays class-based QoS MIB index persistency.
pre-classify	Displays QoS pre-classify events for VPN.
provision	Displays QoS provisions.
service-policy	Displays QoS service policies.
set	Displays QoS packet marking.
snmp	Displays class-based QoS configuration and statistics information.
tunnel_marking	Displays QoS packet tunnel marking.

Command Default

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS 15.0(2)EX	This command was introduced.

Usage Guidelines

The **undebug qos** command is the same as the **no debug qos** 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 (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** *acl-index-or-name*| **ip** {**dscp** *dscp-list* | **precedence** *ip-precedence-list*}| **protocol** {**arp**| **cdp**| **http**| **ip**| **ipv6**}}

no match {**access-group** *acl-index-or-name*| **ip** {**dscp** *dscp-list* | **precedence** *ip-precedence-list*}| **protocol** {**arp**| **cdp**| **http**| **ip**| **ipv6**}}

Syntax Description

access-group *acl-index-or-name*	Specifies the number or name of an access control list (ACL). The range is from 1 to 2799.
ip	Sets IP specific values. • **dscp** *dscp-list*—Lists 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. • **precedence** *ip-precedence-list*—Lists 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.
protocol	Specifies the name of a protocol to be used as the match criteria against which packets are checked to determine if they belong to the class specified by the class map. The following protocols are supported: **arp**,**cdp**, **http**, **ip**, and **ipv6**.

Command Default

No match criteria are defined.

Command Modes

Class-map configuration

Command History

Release	Modification
Cisco IOS 15.0(2)EX	This command was introduced.

Usage Guidelines

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

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

- **match access-group name** *acl-name*
- **match ip dscp** *dscp-list*
- **match ip precedence** *ip-precedence-list*

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

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.

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

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:

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

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

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

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

Related Commands

Command	Description
class-map, on page 44	Creates a class map to be used for matching packets to the class whose name you specify.
show class-map, on page 88	Displays quality of service (QoS) class maps.

mls qos

To enable quality of service (QoS) for the entire switch, use the **mls qos** command in global configuration mode. Use the **no** form of this command to reset all the QoS-related statistics and to disable the QoS features for the entire switch.

mls qos

no mls qos

Syntax Description

This command has no arguments or keywords.

Command Default

QoS is disabled. There is no concept of trusted or untrusted ports because the packets are not modified (the CoS, DSCP, and IP precedence values in the packet are not changed). Traffic is switched in pass-through mode (packets are switched without any rewrites and classified as best effort without any policing).

When QoS is enabled with the **mls qos** global configuration command and all other QoS settings are set to their defaults, traffic is classified as best effort (the DSCP and CoS value is set to 0) without any policing. No policy maps are configured. The default port trust state on all ports is untrusted. The default egress queue settings are in effect.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS 15.0(2)EX	This command was introduced.

Usage Guidelines

When the **mls qos** command is entered, QoS is enabled with the default parameters on all ports in the system.

QoS must be globally enabled to use QoS classification, policing, marking or dropping, queueing, and traffic shaping features. You can create a policy map and attach it to a port before entering the **mls qos** command. QoS processing is disabled until you enter the **mls qos** command.

When you enter the **no mls qos** command, policy maps and class maps that are used to configure QoS are not deleted from the configuration, but entries corresponding to policy maps are removed from the switch hardware to save system resources. To reenable QoS with the previous configurations, enter the **mls qos** command.

Toggling the QoS status of the switch with this command modifies (reallocates) the sizes of the queues. During the queue size modification, the queue is temporarily shut down during the hardware reconfiguration, and the switch drops newly arrived packets for this queue.

Examples

This example shows how to enable QoS on the switch:

```
Switch(config)# mls qos
```

You can verify your settings by entering the **show mls qos** privileged EXEC command.

Related Commands

Command	Description
show mls qos, on page 89	Displays QoS information.

mls qos aggregate-policer

To define policer parameters that can be shared by multiple classes within the same policy map, use the **mls qos aggregate-policer** command in global configuration mode. Use the **no** form of this command to delete an aggregate policer.

mls qos aggregate-policer *aggregate-policer-name rate-bps burst-byte* **exceed-action** {**drop**| **policed-dscp-transmit**}

no mls qos aggregate-policer *aggregate-policer-name rate-bps burst-byte* {**drop**| **policed-dscp-transmit**}

Syntax Description

aggregate-policer-name	The name of the aggregate policer as referenced by the **police aggregate** policy-map class configuration command.
rate-bps	The average traffic rate in bits per second (b/s). The range is 8000 to 10000000000.
burst-byte	The normal burst size in bytes. The range is 8000 to 1000000.
exceed-action drop	Sets the traffic rate. If the rate is exceeded, the switch drops the packet.
exceed-action policed-dscp-transmit	Sets the traffic rate. If the rate is exceeded, the switch changes the Differentiated Services Code Point (DSCP) of the packet to that specified in the policed-DSCP map and then sends the packet.

Command Default

No aggregate policers are defined.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS 15.0(2)EX	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.

Define an aggregate policer if the policer is shared with multiple classes.

Policers for a port cannot be shared with other policers for another port; traffic from two different ports cannot be aggregated for policing purposes.

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).

You apply an aggregate policer to multiple classes in the same policy map; you cannot use an aggregate policer across different policy maps.

You cannot delete an aggregate policer if it is being used in a policy map. You must first use the **no police aggregate** *aggregate-policer-name* policy-map class configuration command to delete the aggregate policer from all policy maps before using the **no mls qos aggregate-policer** *aggregate-policer-name* 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 fast (the average rate) that 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 define the aggregate policer parameters and how to apply the policer to multiple classes in a policy map:

```
Switch(config)# mls qos aggregate-policer agg_policer1 1000000 1000000 exceed-action drop
Switch(config)# policy-map policy2
Switch(config-pmap)# class class1
Switch(config-pmap-c)# police aggregate agg_policer1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class2
Switch(config-pmap-c)# set dscp 10
Switch(config-pmap-c)# police aggregate agg_policer1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class3
Switch(config-pmap-c)# trust dscp
Switch(config-pmap-c)# police aggregate agg_policer2
Switch(config-pmap-c)# exit
```

You can verify your settings by entering the **show mls qos aggregate-policer** privileged EXEC command.

Related Commands

Command	Description
police aggregate, on page 78	Creates a policer that is shared by different classes.
show mls qos aggregate-policer, on page 90	Displays the quality of service (QoS) aggregate policer configuration.

mls qos cos

To define the default class of service (CoS) value of a port or to assign the default CoS to all incoming packets on the port, use the **mls qos cos** command in interface configuration mode. Use the **no** form of this command to return to the default setting.

mls qos cos {*default-cos*| **override**}

no qos mls cos {*default-cos*| **override**}

Syntax Description

default-cos	The default CoS value that is assigned to a port. If packets are untagged, the default CoS value becomes the packet CoS value. The CoS range is 0 to 7.
override	Overrides the CoS value of the incoming packets, and apply the default CoS value on the port to all incoming packets.

Command Default

The default CoS value for a port is 0.

CoS override is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS 15.0(2)EX	This command was introduced.

Usage Guidelines

You can use the default value to assign a CoS and Differentiated Services Code Point (DSCP) value to all incoming packets that are untagged (if the incoming packet does not have a CoS value). You also can assign a default CoS and DSCP value to all incoming packets by using the **override** keyword.

Use the **override** keyword when all incoming packets on certain ports deserve higher or lower priority than packets entering from other ports. Even if a port is previously set to trust DSCP, CoS, or IP precedence, this command overrides the previously configured trust state, and all the incoming CoS values are assigned the default CoS value configured with the **mls qos cos** command. If an incoming packet is tagged, the CoS value of the packet is modified with the default CoS of the port at the ingress port.

Examples

This example shows how to configure the default port CoS to 4 on a port:

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# mls qos trust cos
Switch(config-if)# mls qos cos 4
```

This example shows how to assign all the packets entering a port to the default port CoS value of 4 on a port:

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# mls qos cos 4
Switch(config-if)# mls qos cos override
```

You can verify your settings by entering the **show mls qos interface** privileged EXEC command.

Related Commands

Command	Description
show mls qos interface, on page 91	Displays quality of service (QoS) information.

mls qos dscp-mutation

To apply a Differentiated Services Code Point (DSCP)-to-DSCP-mutation map to a DSCP-trusted port, use the **mls qos dscp-mutation** command in interface configuration mode. Use the **no** form of this command to return the map to the default settings.

mls qos dscp-mutation *dscp-mutation-name*

no mls qos dscp-mutation *dscp-mutation-name*

Syntax Description

dscp-mutation-name	The name of the DSCP-to-DSCP-mutation map. This map was previously defined with the **mls qos map dscp-mutation** global configuration command.

Command Default

The default DSCP-to-DSCP-mutation map is a null map, which maps incoming DSCPs to the same DSCP values.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS 15.0(2)EX	This command was introduced.

Usage Guidelines

If two quality of service (QoS) domains have different DSCP definitions, use the DSCP-to-DSCP-mutation map to translate one set of DSCP values to match the definition of another domain. You apply the DSCP-to-DSCP-mutation map to the receiving port (ingress mutation) at the boundary of a QoS administrative domain.

With ingress mutation, the new DSCP value overwrites the one in the packet, and QoS handles the packet with this new value. The switch sends the packet out the port with the new DSCP value.

You can configure multiple DSCP-to-DSCP-mutation maps on ingress ports.

You apply the map only to DSCP-trusted ports. If you apply the DSCP mutation map to an untrusted port, to CoS or IP-precedence trusted port, the command has no immediate effect until the port becomes DSCP-trusted.

Examples

This example shows how to define the DSCP-to-DSCP mutation map named *dscpmutation1* and to apply the map to a port:

```
Switch(config)# mls qos map dscp-mutation dscpmutation1 10 11 12 13 to 30
Switch(config)# interface gigabitethernet3/0/1
Switch(config-if)# mls qos trust dscp
Switch(config-if)# mls qos dscp-mutation dscpmutation1
```

This example shows how to remove the DSCP-to-DSCP mutation map name *dscpmutation1* from the port and to reset the map to the default:

```
Switch(config-if)# no mls qos dscp-mutation dscpmutation1
```

You can verify your settings by entering the **show mls qos maps** privileged EXEC command.

Related Commands

Command	Description
mls qos map, on page 58	Defines the DSCP-to-DSCP mutation map.
mls qos trust, on page 73	Configures the port trust state.
show mls qos maps, on page 95	Displays QoS mapping information.

mls qos map

To define the class of service (CoS)-to-Differentiated Services Code Point (DSCP) map, DSCP-to-CoS map, the DSCP-to-DSCP-mutation map, the IP-precedence-to-DSCP map, and the policed-DSCP map, use the **mls qos map** command in global configuration mode. Use the **no** form of this command to return to the default map.

mls qos map {**cos-dscp** *dscp1 ... dscp8*| **dscp-cos** *dscp-list to cos*| **dscp-mutation** *dscp-mutation-name in-dscp* **to** *out-dscp*| **ip-prec-dscp** *dscp1 ... dscp8*| **policed-dscp** *dscp-list* **to** *mark-down-dscp*}

no mls qos map {**cos-dscp** *dscp1 ... dscp8*| **dscp-cos** *dscp-list to cos*| **dscp-mutation** *dscp-mutation-name in-dscp* **to** *out-dscp*| **ip-prec-dscp** *dscp1 ... dscp8*| **policed-dscp** *dscp-list* **to** *mark-down-dscp*}

Syntax Description

cos-dscp *dscp1...dscp8*	Defines the CoS-to-DSCP map. For *dscp1...dscp8*, enter eight DSCP values that correspond to CoS values 0 to 7. Separate each DSCP value with a space. The range is 0 to 63.
dscp-cos *dscp-list* **to** *cos*	Defines the DSCP-to-CoS map. For *dscp-list*, enter up to eight DSCP values, with each value separated by a space, then enter the **to** keyword. The range is 0 to 63. For *cos*, enter a single CoS value to which the DSCP values correspond. The range is 0 to 7.
dscp-mutation *dscp-mutation-name in-dscp* **to** *out-dscp*	Defines the DSCP-to-DSCP-mutation map. For *dscp-mutation-name*, enter the mutation map name. For *in-dscp*, enter up to eight DSCP values, with each value separated by a space, then enter the **to** keyword. For *out-dscp*, enter a single DSCP value. The range is 0 to 63.
ip-prec-dscp *dscp1...dscp8*	Defines the IP-precedence-to-DSCP map. For *dscp1...dscp8*, enter eight DSCP values that correspond to the IP precedence values 0 to 7. Separate each DSCP value with a space. The range is 0 to 63.
policed-dscp *dscp-list* **to** *mark-down-dscp*	Defines the policed-DSCP map. For *dscp-list*, enter up to eight DSCP values, with each value separated by a space, then enter the **to** keyword. For *mark-down-dscp*, enter the corresponding policed (marked down) DSCP value. The range is 0 to 63.

Command Default

- For the default CoS-to-DSCP map, see Table 11: Default CoS-to-DSCP Map, on page 59.
- For the default DSCP-to-CoS map, see Table 12: Default DSCP-to-CoS Map, on page 60.
- For the default IP-precedence-to-DSCP map, see Table 13: Default IP-Precedence-to-DSCP Map, on page 60.

When this command is disabled, the default maps are set.

The default DSCP-to-DSCP-mutation map is a null map, which maps an incoming DSCP value to the same DSCP value.

The default policed-DSCP map is a null map, which maps an incoming DSCP value to the same DSCP value.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS 15.0(2)EX	This command was introduced.

Usage Guidelines

All the maps are globally defined. All the maps, except the DSCP-to-DSCP-mutation map, are applied to all ports. The DSCP-to-DSCP-mutation map is applied to a specific port.

Table 11: Default CoS-to-DSCP Map

CoS Value	DSCP Value
0	0
1	8
2	16
3	24
4	32
5	40
6	48
7	56

Table 12: Default DSCP-to-CoS Map

DSCP Value	CoS Value
0–7	0
8–15	1
16–23	2
24–31	3
32–39	4
40–47	5
48–55	6
56–63	7

Table 13: Default IP-Precedence-to-DSCP Map

IP Precedence Value	DSCP Value
0	0
1	8
2	16
3	24
4	32
5	40
6	48
7	56

Examples

This example shows how to define the IP-precedence-to-DSCP map and to map IP-precedence values 0 to 7 to DSCP values of 0, 10, 20, 30, 40, 50, 55, and 60:

```
Switch# configure terminal
Switch(config)# mls qos map ip-prec-dscp 0 10 20 30 40 50 55 60
```

This example shows how to define the policed-DSCP map. DSCP values 1, 2, 3, 4, 5, and 6 are marked down to DSCP value 0. Marked DSCP values that not explicitly configured are not modified:

```
Switch# configure terminal
Switch(config)# mls qos map policed-dscp 1 2 3 4 5 6 to 0
```

This example shows how to define the DSCP-to-CoS map. DSCP values 20, 21, 22, 23, and 24 are mapped to CoS 1. DSCP values 10, 11, 12, 13, 14, 15, 16, and 17 are mapped to CoS 0:

```
Switch# configure terminal
Switch(config)# mls qos map dscp-cos 20 21 22 23 24 to 1
Switch(config)# mls qos map dscp-cos 10 11 12 13 14 15 16 17 to 0
```

This example shows how to define the CoS-to-DSCP map. CoS values 0 to 7 are mapped to DSCP values 0, 5, 10, 15, 20, 25, 30, and 35:

```
Switch# configure terminal
Switch(config)# mls qos map cos-dscp 0 5 10 15 20 25 30 35
```

This example shows how to define the DSCP-to-DSCP-mutation map. All the entries that are not explicitly configured are not modified (remain as specified in the null map):

```
Switch# configure terminal
Switch(config)# mls qos map dscp-mutation mutation1 1 2 3 4 5 6 7 to 10
Switch(config)# mls qos map dscp-mutation mutation1 8 9 10 11 12 13 to 10
Switch(config)# mls qos map dscp-mutation mutation1 20 21 22 to 20
Switch(config)# mls qos map dscp-mutation mutation1 0 31 32 33 34 to 30
```

You can verify your settings by entering the **show mls qos maps** privileged EXEC command.

Related Commands

Command	Description
mls qos dscp-mutation, on page 56	Applies a DSCP-to-DSCP-mutation map to a DSCP-trusted port.
show mls qos maps, on page 95	Displays quality of service (QoS) mapping information.

mls qos queue-set output buffers

To allocate buffers to a queue set of four egress queues per port, use the **mls qos queue-set output buffers** command in global configuration mode. To return to the default setting, use the **no** form of this command.

mls qos queue-set output *qset-id* **buffers** *allocation1 ... allocation4*

no mls qos queue-set output *qset-id* **buffers**

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.
allocation1 ... allocation4	Buffer space allocation (percentage) for each queue (four values for queues 1 to 4). For *allocation1*, *allocation3*, and *allocation4*, the range is 0 to 99. For *allocation2*, the range is 1 to 100 (including the CPU buffer). Separate each value with a space.

Command Default

All allocation values are equally mapped among the four queues (25, 25, 25, 25). Each queue has 1/4th of the buffer space.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS 15.0(2)EX	This command was introduced.

Usage Guidelines

Specify the allocation values, and separate each with a space.

Allocate buffers according to the importance of the traffic. For example, give a large percentage of the buffer to the queue with the highest-priority traffic.

Note The egress queue default settings are suitable for most situations. Change them only when you have a thorough understanding of the egress queues and if these settings do not meet your QoS solution.

To configure different classes of traffic with different characteristics, use this command with the **mls qos queue-set output** *qset-id* **threshold** global configuration command.

Examples

This example shows how to map a port to queue set *2*. It allocates 40 percent of the buffer space to egress queue 1 and 20 percent to egress queues 2, 3, and 4.

```
Switch(config)# mls qos queue-set output 2 buffers 40 20 20 20
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# queue-set 2
```

You can verify your settings by entering the **show mls qos interface** [*interface-id* **buffers**] or the **show mls qos queue-set** privileged EXEC command.

Related Commands

Command	Description
mls qos queue-set output threshold, on page 64	Configures the weighted tail-drop (WTD) thresholds, guarantees the availability of buffers, and configures the maximum memory allocation to a queue set.
queue-set, on page 82	Maps a port to a queue set.
show mls qos interface, on page 91	Displays quality of service (QoS) information at the port level
show mls qos queue-set, on page 98	Displays egress queue settings for the queue set.

mls qos queue-set output threshold

To configure the weighted tail-drop (WTD) thresholds, to guarantee the availability of buffers, and to configure the maximum memory allocation to a queue set (four egress queues per port), use the **mls qos queue-set output threshold** command in global configuration mode. Use the **no** form of this command to return to the default setting.

mls qos queue-set output *qset-id* **threshold** [*queue-id*] *drop-threshold1 drop-threshold2 reserved-threshold maximum-threshold*

no mls qos queue-set output *qset-id* **threshold** [*queue-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.
queue-id	(Optional) The queue in the queue set on which the command is performed. The range is 1 to 4.
drop-threshold1 *drop-threshold2*	Two WTD thresholds expressed as a percentage of the allocated memory of the queue. The range is 1 to 3200 percent.
reserved-threshold	The amount of memory to be guaranteed (reserved) for the queue and expressed as a percentage of the allocated memory. The range is 1 to 100 percent.
maximum-threshold	Queue in the full condition that is enabled to get more buffers than are reserved for it. This is the maximum memory the queue can have before the packets are dropped. The range is 1 to 3200 percent.

Command Default

When quality of service (QoS) is enabled, WTD is enabled.

For default egress queue WTD threshold values , see Table 14: Default Egress Queue WTD Threshold Settings, on page 65.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS 15.0(2)EX	This command was introduced.

Usage Guidelines

Use the **mls qos queue-set output** *qset-id* **buffers** global configuration command to allocate a fixed number of buffers to the four queues in a queue set.

Table 14: Default Egress Queue WTD Threshold Settings

Feature	Queue 1	Queue 2	Queue 3	Queue 4
WTD drop threshold 1	100 percent	200 percent	100 percent	100 percent
WTD drop threshold 2	100 percent	200 percent	100 percent	100 percent
Reserved threshold	50 percent	100 percent	50 percent	50 percent
Maximum threshold	400 percent	400 percent	400 percent	400 percent

The drop-threshold percentages can exceed 100 percent and can be up to the maximum (if the maximum threshold exceeds 100 percent).

While buffer ranges allow individual queues in the queue set to use more of the common pool when available, the maximum user-configurable number of packets for each queue is still internally limited to 3200 percent, or 32 times the allocated number of buffers. One packet can use one 1 or more buffers.

Note The egress queue default settings are suitable for most situations. Change them only when you have a thorough understanding of the egress queues and if these settings do not meet your QoS solution.

The switch uses a buffer allocation scheme to reserve a minimum amount of buffers for each egress queue, to prevent any queue or port from consuming all the buffers and depriving other queues, and to decide whether to grant buffer space to a requesting queue. The switch decides whether the target queue has not consumed more buffers than its reserved amount (under-limit), whether it has consumed all of its maximum buffers (over-limit), and whether the common pool is empty (no free buffers) or not empty (free buffers). If the queue is not over-limit, the switch can allocate buffer space from the reserved pool or from the common pool (if it is not empty). If there are no free buffers in the common pool or if the queue is over-limit, the switch drops the frame.

Examples

This example shows how to map a port to queue set 2. It configures the drop thresholds for queue 2 to 40 and 60 percent of the allocated memory, guarantees (reserves) 100 percent of the allocated memory, and configures 200 percent as the maximum memory this queue can have before packets are dropped:

```
Switch(config)# mls qos queue-set output 2 threshold 2 40 60 100 200
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# queue-set 2
```

You can verify your settings by entering the **show mls qos interface** [*interface-id*] **buffers** or the **show mls qos queue-set** privileged EXEC command.

Related Commands

Command	Description
mls qos queue-set output buffers, on page 62	Allocates buffers to a queue set.

Command	Description
queue-set, on page 82	Maps a port to a queue set.
show mls qos interface, on page 91	Displays quality of service (QoS) information at the port level.
show mls qos queue-set, on page 98	Displays egress queue settings for the queue-set.

mls qos rewrite ip dscp

To configure the switch to change or rewrite the Differentiated Services Code Point (DSCP) field of an incoming IP packet, use the **mls qos rewrite ip dscp** command in global configuration mode. Use the **no** form of this command to configure the switch to not modify or rewrite the DSCP field of the packet and to enable DSCP transparency.

mls qos rewrite ip dscp

no mls qos rewrite ip dscp

Syntax Description

This command has no arguments or keywords.

Command Default

DSCP transparency is disabled. The switch changes the DSCP field of the incoming IP packet.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS 15.0(2)EX	This command was introduced.

Usage Guidelines

DSCP transparency affects only the DSCP field of a packet at the egress. If DSCP transparency is enabled by using the **no mls qos rewrite ip dscp** command, the switch does not modify the DSCP field in the incoming packet, and the DSCP field in the outgoing packet is the same as that in the incoming packet.

Note Enabling DSCP transparency does not affect the port trust settings on IEEE 802.1Q tunneling ports.

By default, DSCP transparency is disabled. The switch modifies the DSCP field in an incoming packet, and the DSCP field in the outgoing packet is based on the quality of service (QoS) configuration, including the port trust setting, policing and marking, and the DSCP-to-DSCP mutation map.

Regardless of the DSCP transparency configuration, the switch modifies the internal DSCP value of the packet that the switch uses to generate a class of service (CoS) value representing the priority of the traffic. The switch also uses the internal DSCP value to select an egress queue and threshold.

For example, if QoS is enabled and an incoming packet has a DSCP value of 32, the switch might modify the internal DSCP value based on the policy-map configuration and change the internal DSCP value to 16. If DSCP transparency is enabled, the outgoing DSCP value is 32 (same as the incoming value). If DSCP transparency is disabled, the outgoing DSCP value is 16 because it is based on the internal DSCP value.

Examples

This example shows how to enable DSCP transparency and configure the switch to not change the DSCP value of the incoming IP packet:

```
Switch(config)# mls qos
Switch(config)# no mls qos rewrite ip dscp
```

This example shows how to disable DSCP transparency and configure the switch to change the DSCP value of the incoming IP packet:

```
Switch(config)# mls qos
Switch(config)# mls qos rewrite ip dscp
```

You can verify your settings by entering the **show running config include rewrite** privileged EXEC command.

Related Commands

Command	Description
mls qos, on page 50	Enables QoS globally.
show mls qos, on page 89	Displays QoS information.
show running-config | include rewrite	Displays the DSCP transparency setting.

mls qos srr-queue output cos-map

To map class of service (CoS) values to an egress queue or to map CoS values to a queue and to a threshold ID, use the **mls qos srr-queue output cos-map** command global configuration mode. Use the **no** form of this command to return to the default setting.

mls qos srr-queue output cos-map queue *queue-id* {*cos1 ... cos8* | **threshold** *threshold-id cos1 ... cos8* }

no mls qos srr-queue output cos-map

Syntax Description

queue *queue-id*	Specifies a queue number. For *queue-id*, the range is 1 to 4.
cos1 ... cos8	CoS values that are mapped to an egress queue. For *cos1...cos8*, enter up to eight values, and separate each value with a space. The range is 0 to 7.
threshold *threshold-id cos1...cos8*	Maps CoS values to a queue threshold ID. For *threshold-id*, the range is 1 to 3. For *cos1...cos8*, enter up to eight values, and separate each value with a space. The range is 0 to 7.

Command Default

For default CoS output queue thresholds values, see Table 15: Default Cos Output Queue Threshold Map, on page 70.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS 15.0(2)EX	This command was introduced.

Usage Guidelines

The drop-threshold percentage for threshold 3 is predefined. It is set to the queue-full state.

Note The egress queue default settings are suitable for most situations. Change them only when you have a thorough understanding of the egress queues and if these settings do not meet your quality of service (QoS) solution.

You can assign two weighted tail-drop (WTD) threshold percentages to an egress queue by using the **mls qos queue-set output** *qset-id* **threshold** global configuration command.

You can map each CoS value to a different queue and threshold combination, allowing the frame to follow different behavior.

Table 15: Default Cos Output Queue Threshold Map

CoS Value	0	1	2	3	4	5	6	7
Queue ID–Threshold ID	2–1	2–1	3–1	3–1	4–1	1–1	4–1	4–1

Examples

This example shows how to map a port to queue set 1. It maps CoS values 0 to 3 to egress queue 1 and to threshold ID 1. It configures the drop thresholds for queue 1 to 50 and 70 percent of the allocated memory, guarantees (reserves) 100 percent of the allocated memory, and configures 200 percent as the maximum memory that this queue can have before packets are dropped.

```
Switch(config)# mls qos srr-queue output cos-map queue 1 threshold 1 0 1 2 3
Switch(config)# mls qos queue-set output 1 threshold 1 50 70 100 200
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# queue-set 1
```

You can verify your settings by entering the **show mls qos maps**, the **show mls qos interface** [*interface-id*] **buffers**, or the **show mls qos queue-set** privileged EXEC command.

Related Commands

Command	Description
mls qos queue-set output threshold, on page 64	Configures the WTD thresholds, guarantees the availability of buffers, and configures the maximum memory allocation to a queue-set.
mls qos srr-queue output dscp-map, on page 71	Maps Differentiated Services Code Point (DSCP) values to an egress queue or maps DSCP values to a queue and to a threshold ID.
queue-set, on page 82	Maps a port to a queue set.
show mls qos interface, on page 91	Displays quality of service (QoS) information at the port level
show mls qos maps, on page 95	Displays QoS mapping information.
show mls qos queue-set, on page 98	Displays egress queue settings for the queue-set.

mls qos srr-queue output dscp-map

To map Differentiated Services Code Point (DSCP) values to an egress queue or to map DSCP values to a queue and to a threshold ID, use the **mls qos srr-queue output dscp-map** command in global configuration mode. Use the **no** form of this command to return to the default setting.

mls qos srr-queue output dscp-map queue *queue-id* { *dscp1 ... dscp8* | **threshold** *threshold-id dscp1 ... dscp8* }

no mls qos srr-queue output dscp-map

Syntax Description

queue *queue-id*	Specifies a queue number. For *queue-id*, the range is 1 to 4.
dscp1 ... dscp8	DSCP values that are mapped to an egress queue. For *dscp1...dscp8*, enter up to eight values, and separate each value with a space. The range is 0 to 63.
threshold *threshold-id dscp1...dscp8*	Maps DSCP values to a queue threshold ID. For *threshold-id*, the range is 1 to 3. For *dscp1...dscp8*, enter up to eight values, and separate each value with a space. The range is 0 to 63.

Command Default

The default DSCP output queue thresholds are set.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS 15.0(2)EX	This command was introduced.

Usage Guidelines

The drop-threshold percentage for threshold 3 is predefined. It is set to the queue-full state.

For default DSCP output queue-threshold map values, see Table 16: Default DSCP Output Queue Threshold Map, on page 72.

Note The egress queue default settings are suitable for most situations. Change them only when you have a thorough understanding of the egress queues and if these settings do not meet your QoS solution.

You can assign two weighted tail-drop (WTD) threshold percentages to an egress queue by using the **mls qos queue-set output** *qset-id* **threshold** global configuration command.

You can map each DSCP value to a different queue and threshold combination, allowing the frame to follow different behavior.

You can map up to eight DSCP values per command.

Table 16: Default DSCP Output Queue Threshold Map

DSCP Value	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
Queue ID–Threshold ID	2–1	2–1	3–1	3–1	4–1	1–1	4–1	4–1

Examples

This example shows how to map a port to queue set 1. It maps DSCP values 0 to 3 to egress queue 1 and to threshold ID 1. It configures the drop thresholds for queue 1 to 50 and 70 percent of the allocated memory, guarantees (reserves) 100 percent of the allocated memory, and configures 200 percent as the maximum memory that this queue can have before packets are dropped.

```
Switch(config)# mls qos srr-queue output dscp-map queue 1 threshold 1 0 1 2 3
Switch(config)# mls qos queue-set output 1 threshold 1 50 70 100 200
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# queue-set 1
```

You can verify your settings by entering the **show mls qos maps**, the **show mls qos interface** [*interface-id*] **buffers** or the **show mls qos queue-set** privileged EXEC command.

Related Commands

Command	Description
mls qos srr-queue output cos-map, on page 69	Maps class of service (CoS) values to an egress queue or maps CoS values to a queue and to a threshold ID.
mls qos queue-set output threshold, on page 64	Configures the WTD thresholds, guarantees the availability of buffers, and configures the maximum memory allocation to a queue-set.
queue-set, on page 82	Maps a port to a queue set.
show mls qos interface, on page 91	Displays quality of service (QoS) information at the port level
show mls qos maps, on page 95	Displays QoS mapping information.
show mls qos queue-set, on page 98	Displays egress queue settings for the queue set.

mls qos trust

To configure the port trust state, use the **mls qos trust** command in interface configuration mode. Use the **no** form of this command to return a port to its untrusted state.

mls qos trust [**cos**| **device** {**cisco-phone**| **cts**| **ip-camera**| **media-player**}| **dscp**| **ip-precedence**]

no mls qos trust [**cos**| **device** {**cisco-phone**| **cts**| **ip-camera**| **media-player**}| **dscp**| **ip-precedence**]

Syntax Description

cos	(Optional) Classifies an ingress packet by using the packet CoS value. For an untagged packet, use the port default CoS value.
device cisco-phone	(Optional) Classifies an ingress packet by trusting the CoS or DSCP value sent from the Cisco IP Phone (trusted boundary), depending on the trust setting.
device {**cts** | **ip-camera** | **media-player**}	(Optional) Classifies an ingress packet by trusting the CoS or DSCP value for these video devices: • **cts—**Cisco TelePresence System • **ip-camera—**Cisco IP camera • **media-player—**Cisco digital media player For an untagged packet, use the port default CoS value.
dscp	(Optional) Classifies an ingress packet by using the packet DSCP value (most significant 6 bits of 8-bit service-type field). For a non-IP packet, the packet CoS is used if the packet is tagged. For an untagged packet, the default port CoS value is used.
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 is used if the packet is tagged. For an untagged packet, the port default CoS value is used.

Command Default

The port is not trusted. If no keyword is specified when you enter the command, the default is **dscp**.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS 15.0(2)EX	This command was introduced.

Usage Guidelines

Packets entering a quality of service (QoS) domain are classified at the edge of the domain. When the packets are classified at the edge, the switch port within the QoS domain can be configured to one of the trusted states because there is no need to classify the packets at every switch within the domain. Use this command to specify whether the port is trusted and which fields of the packet to use to classify traffic.

When a port is configured with trust DSCP or trust IP precedence and the incoming packet is a non-IP packet, the CoS-to-DSCP map is used to derive the corresponding DSCP value from the CoS value. The CoS can be the packet CoS for trunk ports or the port default CoS for nontrunk ports.

If the DSCP is trusted, the DSCP field of the IP packet is not modified. However, it is still possible that the CoS value of the packet is modified (according to DSCP-to-CoS map).

If the CoS is trusted, the CoS field of the packet is not modified, but the DSCP can be modified (according to CoS-to-DSCP map) if the packet is an IP packet.

The trusted boundary feature prevents security problems if users disconnect their PCs from networked Cisco IP Phones and connect them to the switch port to take advantage of trusted CoS or DSCP settings. You must globally enable the Cisco Discovery Protocol (CDP) on the switch and on the port connected to the IP phone. If the telephone is not detected, trusted boundary disables the trusted setting on the switch or routed port and prevents misuse of a high-priority queue.

If you configure the trust setting for DSCP or IP precedence, the DSCP or IP precedence values in the incoming packets are trusted. If you configure the **mls qos cos override** interface configuration command on the switch port connected to the IP phone, the switch overrides the CoS of the incoming voice and data packets and assigns the default CoS value to them.

For an inter-QoS domain boundary, you can configure the port to the DSCP-trusted state and apply the DSCP-to-DSCP-mutation map if the DSCP values are different between the QoS domains.

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.

Related Commands

This example shows how to configure a port to trust the IP precedence field in the incoming packet:

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# mls qos trust ip-precedence
```

This example shows how to specify that the Cisco IP Phone connected on a port is a trusted device:

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# mls qos trust device cisco-phone
```

You can verify your settings by entering the **show mls qos interface** privileged EXEC command.

Related Commands

Command	Description
mls qos cos, on page 54	Defines the default CoS value of a port or assigns the default CoS to all incoming packets on the port.
mls qos dscp-mutation, on page 56	Applies a DSCP-to DSCP-mutation map to a DSCP-trusted port.

Command	Description
mls qos map, on page 58	Defines the CoS-to-DSCP map, DSCP-to-CoS map, the DSCP-to-DSCP-mutation map, the IP-precedence-to-DSCP map, and the policed-DSCP map.
show mls qos interface, on page 91	Displays QoS information.

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* [**exceed-action** [**drop** | **policed-dscp-transmit**]]

no police *rate-bps burst-byte* [**exceed-action** [**drop** | **policed-dscp-transmit**]]

Syntax Description

rate-bps	Specifies the average traffic rate in bits per second (b/s). The range is 8000 to 10000000000.
burst-byte	Specifies the normal burst size in bytes. The range is 8000 to 1000000.
exceed-action drop	(Optional) Sets the traffic rate. If the rate is exceeded, the switch drops the packet .
exceed-action policed-dscp-transmit	(Optional) Sets the traffic rate. If the rate is exceeded, the switch changes the Differentiated Services Code Point (DSCP) of the packet to that specified in the policed-DSCP map and then sends the packet.
aggregate	Chooses the aggregate policer for the current class.

Command Default

No policers are defined.

Command Modes

Policy-map class configuration

Command History

Release	Modification
Cisco IOS 15.0(2)EX	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.

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.

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

```
Switch(config)# policy-map policy2
Switch(config-pmap)# class class2
Switch(config-pmap-c)# police 1000000 20000 exceed-action policed-dscp-transmit
Switch(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.
class-map, on page 44	Create a class map to be used for matching packets to the class whose name you specify with the **class** command.
mls qos map, on page 58 **policed-dscp**	Applies a policed-DSCP map to a DSCP-trusted port.
policy map, on page 80	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
set, on page 86	Classifies IP traffic by setting a DSCP or IP-precedence value in the packet.
show policy-map, on page 99	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.

police aggregate

To apply an aggregate policer to multiple classes in the same policy map, use the **police aggregate** command in policy-map class configuration mode. Use the **no** form of this command to remove the specified policer.

police aggregate *aggregate-policer-name*

no police aggregate *aggregate-policer-name*

Syntax Description

aggregate-policer-name	The name of the aggregate policer.

Command Default

No aggregate policers are defined.

Command Modes

Policy-map class configuration

Command History

Release	Modification
Cisco IOS 15.0(2)EX	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.

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.

You set aggregate policer parameters by using the **mls qos aggregate-policer** global configuration command. You apply an aggregate policer to multiple classes in the same policy map; you cannot use an aggregate policer across different policy maps.

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

You cannot configure aggregate policers in hierarchical policy maps.

Examples

This example shows how to define the aggregate policer parameters and to apply the policer to multiple classes in a policy map:

```
Switch(config)# mls qos aggregate-policer agg_policer1 10000 1000000 exceed-action drop
Switch(config)# policy-map policy2
Switch(config-pmap)# class class1
Switch(config-pmap-c)# police aggregate agg_policer1
```

```
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class2
Switch(config-pmap-c)# set dscp 10
Switch(config-pmap-c)# police aggregate agg_policer1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class3
Switch(config-pmap-c)# trust dscp
Switch(config-pmap-c)# police aggregate agg_policer2
Switch(config-pmap-c)# exit
```

You can verify your settings by entering the **show mls qos aggregate-policer** privileged EXEC command.

Related Commands

Command	Description
mls qos aggregate-policer, on page 52	Defines policer parameters, which can be shared by multiple classes within a policy map.
show mls qos aggregate-policer, on page 90	Displays the quality of service (QoS) aggregate policer configuration.

policy map

To create or modify a policy map that can be attached to multiple physical ports 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	The 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 15.0(2)EX	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.

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.

You can configure QoS only on physical ports. Configure the QoS settings, such as classification, queueing, and scheduling, and apply the policy map to a port. When configuring QoS on a physical port, you apply a nonhierarchical policy map to a port. A nonhierarchical policy map is the same as the port-based policy maps in the switch.

Examples

This example shows how to create a policy map called *policy1*.

```
Switch(config)# policy-map policy1
```

This example shows how to delete *policymap2*:

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

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

Related Commands

Command	Description
class, on page 41	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 44	Creates a class map to be used for matching packets to the class whose name you specify.
service-policy, on page 84	Applies a policy map to a physical port.
show policy-map, on page 99	Displays QoS policy maps.

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 15.0(2)EX	This command was introduced.

Usage Guidelines

For information about automatic generation of the queue-set ID with the **auto qos voip** command, see the "Usage Guidelines" section for the auto qos voip, on page 26 command.

Examples

This example shows how to map a port to queue-set 2:

```
Switch(config)# interface gigabitethernet2/0/1
Switch(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, on page 62	Allocates buffers to a queue set.
mls qos queue-set output threshold, on page 64	Configures the weighted tail-drop (WTD) thresholds, guarantees the availability of buffers, and configures the maximum memory allocation to a queue set.
show mls qos interface, on page 91	Displays quality of service (QoS) information.

service-policy

To apply a policy map to the input of a physical port, 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*	Applies the specified policy map to the input of a physical port.

Command Default

No policy maps are attached to the port.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS 15.0(2)EX	This command was introduced.

Usage Guidelines

Though visible in the command-line help strings, the **output** keyword is not supported.

Policy maps can be configured on physical ports. 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.

You can apply a policy map to incoming traffic on a physical port. .

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.

Examples

This example shows how to remove *plcmap2* from a physical port:

```
Switch(config)# interface gigabitethernet2/0/2
Switch(config-if)# no service-policy input plcmap2
```

You can verify your settings by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
policy map, on page 80	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.

Command	Description
show policy-map, on page 99	Displays QoS policy maps.
show running-config	Displays the operating configuration.

set

To classify IP traffic by setting a Differentiated Services Code Point (DSCP) or an IP-precedence value in the packet, use the **set** command in policy-map class configuration mode. Use the **no** form of this command to remove traffic classification.

set {**dscp** *new-dscp* | **ip** {**dscp| precedence**}| **precedence** *precedence*}

no set {**dscp** *new-dscp* | **ip** {**dscp| precedence**}| **precedence** *precedence*}

Syntax Description

dscp *new-dscp*	Sets the DSCP value in IPv4 and IPv6 packets. The range is 0 to 63.
ip {**dscp** | **precedence** }	Sets the IP values. • **dscp—**Sets the IP DSCP value. • **precedence—**Sets the IP precedence value.
precedence *new-precedence*	Sets the precedence in IPv4 and IPv6 packets. The range is 0 to 7.

Command Default

No traffic classification is defined.

Command Modes

Policy-map class configuration

Command History

Release	Modification
Cisco IOS 15.0(2)EX	This command was introduced.

Usage Guidelines

If you have used the **set ip dscp** policy-map class configuration command, the switch changes this command to **set dscp** in the switch configuration. If you enter the **set ip dscp** policy-map class configuration command, this setting appears as **set dscp** in the switch configuration.

You can use the **set ip precedence** policy-map class configuration command or the **set precedence** policy-map class configuration command. This setting appears as **set ip precedence** in the switch configuration.

The **set** command is mutually exclusive with the **trust** policy-map class configuration command within the same policy map.

For the **set dscp** *new-dscp* or the **set ip precedence** *new-precedence* command, you can enter a mnemonic name for a commonly used value. For example, you can enter the **set dscp af11** command, which is the same as entering the **set dscp 10** command. You can enter the **set ip precedence critical** command, which is the

same as entering the **set ip precedence 5** command. For a list of supported mnemonics, enter the **set dscp ?** or the **set ip precedence ?** command to see the command-line help strings.

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

Examples

This example shows how to assign DSCP 10 to all FTP traffic without any policers:

```
Switch(config)# policy-map policy_ftp
Switch(config-pmap)# class-map ftp_class
Switch(config-cmap)# exit
Switch(config)# policy-map policy_ftp
Switch(config-pmap)# class ftp_class
Switch(config-pmap-c)# set dscp 10
Switch(config-pmap)# exit
```

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

Related Commands

Command	Description
class, on page 41	Defines a traffic classification match criteria (through the **police**, **set**, and **trust** policy-map class configuration commands) for the specified class-map name.
police, on page 76	Defines a policer for classified traffic.
policy map, on page 80	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
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 99	Displays QoS policy maps.
trust, on page 106	Defines a trust state for traffic classified through the **class** policy-map configuration command or the **class-map** global configuration command.

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 15.0(2)EX	This command was introduced.

Usage Guidelines

This command is supported only on the LAN Base image.

Examples

This is an example of output from the **show class-map** command:

```
Switch# 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, on page 44	Creates a class map to be used for matching packets to the class whose name you specify.
match (class-map configuration), on page 48	Defines the match criteria to classify traffic.

show mls qos

To display global quality of service (QoS) configuration information, use the **show mls qos** command in EXEC mode.

show mls qos

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS 15.0(2)EX	This command was introduced.

Examples

This is an example of output from the **show mls qos** command when QoS is enabled and Differentiated Services Code Point (DSCP) transparency is disabled:

```
Switch# show mls qos
QoS is enabled
QoS ip packet dscp rewrite is disabled
```

This is an example of output from the **show mls qos** command when QoS is enabled and DSCP transparency is enabled:

```
Switch# show mls qos
QoS is enabled
QoS ip packet dscp rewrite is enabled
```

Related Commands

Command	Description
mls qos, on page 50	Enables QoS on the entire switch.

show mls qos aggregate-policer

To display the quality of service (QoS) aggregate policer configuration, use the **show mls qos aggregate-policer** command in EXEC mode.

show mls qos aggregate-policer [*aggregate-policer-name*]

Syntax Description

aggregate-policer-name	(Optional) Displays the policer configuration for the specified name.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS 15.0(2)EX	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.

This command is supported only on the LAN Base image.

Examples

This is an example of output from the **show mls qos aggregate-policer** command:

```
Switch# show mls qos aggregate-policer policer1

aggregate-policer policer1 1000000 2000000 exceed-action drop
Not used by any policy map
```

Related Commands

Command	Description
mls qos aggregate-policer, on page 52	Defines policer parameters that can be shared by multiple classes within a policy map.

show mls qos interface

To display quality of service (QoS) information at the port level, use the **show mls qos interface** command in EXEC mode.

show mls qos interface [*interface-id*] [**buffers**| **queueing**| **statistics**]

Syntax Description

interface-id	(Optional) The QoS information for the specified port. Valid interfaces include physical ports.
buffers	(Optional) Displays the buffer allocation among the queues.
queueing	(Optional) Displays the queueing strategy (shared or shaped) and the weights corresponding to the queues.
statistics	(Optional) Displays statistics for sent and received Differentiated Services Code Points (DSCPs) and class of service (CoS) values, the number of packets enqueued or dropped per egress queue, and the number of in-profile and out-of-profile packets for each policer.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS 15.0(2)EX	This command was introduced.

Usage Guidelines

Though visible in the command-line help string, the **policers** keyword is not supported.

This command is supported only on the LAN Base image.

Examples

This is an example of output from the **show mls qos interface** *interface-id* command when port-based QoS is enabled:

```
Switch# show mls qos interface gigabitethernet1/0/1
GigabitEthernet1/0/1
trust state: trust cos
trust mode: trust cos
trust enabled flag: ena
COS override: dis
default COS: 0
DSCP Mutation Map: Default DSCP Mutation Map
Trust device: none
```

```
qos mode: port-based
```

This is an example of output from the **show mls qos interface** *interface-id* command when port-based QoS is disabled:

```
Switch# show mls qos interface  gigabitethernet1/0/1
GigabitEthernet1/0/1
QoS is disabled. When QoS is enabled, following settings will be applied
trust state: trust cos
trust mode: trust cos
trust enabled flag: ena
COS override: dis
default COS: 0
DSCP Mutation Map: Default DSCP Mutation Map
Trust device: none
qos mode: port-based
```

This is an example of output from the **show mls qos interface** *interface-id* **buffers** command:

```
Switch# show mls qos interface gigabitethernet1/0/2 buffers
GigabitEthernet1/0/2
The port is mapped to qset : 1
The allocations between the queues are : 25 25 25 25
```

This is an example of output from the **show mls qos interface** *interface-id* **queueing** command. The egress expedite queue overrides the configured shaped round robin (SRR) weights.

```
Switch# show mls qos interface gigabitethernet1/0/2 queueing
GigabitEthernet1/0/2
Egress Priority Queue :enabled
Shaped queue weights (absolute) :  25 0 0 0
Shared queue weights  :  25 25 25 25
The port bandwidth limit : 100  (Operational Bandwidth:100.0)
The port is mapped to qset : 1
```

This is an example of output from the **show mls qos interface** *interface-id* **statistics** command:

```
Switch# show mls qos interface gigabitethernet1/0/1 statistics
GigabitEthernet1/0/1 (All statistics are in packets)

  dscp: incoming
-------------------------------

  0 -  4 :       15233            0            0            0            0
  5 -  9 :           0            0            0            0            0
 10 - 14 :           0            0            0            0            0
 15 - 19 :           0            0            0            0            0
 20 - 24 :           0            0            0            0            0
 25 - 29 :           0            0            0            0            0
 30 - 34 :           0            0            0            0            0
 35 - 39 :           0            0            0            0            0
 40 - 44 :           0            0            0            0            0
 45 - 49 :           0            0            0       406417            0
 50 - 54 :           0            0            0            0            0
 55 - 59 :           0            0            0            0            0
 60 - 64 :           0            0            0            0
  dscp: outgoing
-------------------------------

  0 -  4 :         337            0            0            0            0
  5 -  9 :           0            0            0            0            0
 10 - 14 :           0            0            0            0            0
 15 - 19 :           0            0            0            0            0
 20 - 24 :           0            0            0            0            0
 25 - 29 :           0            0            0            0            0
 30 - 34 :           0            0            0            0            0
 35 - 39 :           0            0            0            0            0
 40 - 44 :           0            0            0            0            0
 45 - 49 :           0            0            0        13866            0
 50 - 54 :           0            0            0            0            0
 55 - 59 :           0            0            0            0            0
 60 - 64 :           0            0            0            0
```

```
  cos: incoming
-------------------------------

  0 -  4 :     1426270            0            0            0            0
  5 -  7 :           0            0            0
  cos: outgoing
-------------------------------

  0 -  4 :      131687           12            0            0         7478
  5 -  7 :        1993        25483       275213
  output queues enqueued:
 queue:    threshold1   threshold2   threshold3
-----------------------------------------------
 queue 0:           0            0            0
 queue 1:           0          341       441525
 queue 2:           0            0            0
 queue 3:           0            0            0

  output queues dropped:
 queue:    threshold1   threshold2   threshold3
-----------------------------------------------
 queue 0:           0            0            0
 queue 1:           0            0            0
 queue 2:           0            0            0
 queue 3:           0            0            0

Policer: Inprofile:            0 OutofProfile:            0
```

This table describes the fields in this display.

Table 17: show mls qos interface statistics Field Descriptions

Field		Description
DSCP	incoming	Number of packets received for each DSCP value.
	outgoing	Number of packets sent for each DSCP value.
CoS	incoming	Number of packets received for each CoS value.
	outgoing	Number of packets sent for each CoS value.
Output queues	enqueued	Number of packets in the egress queue.
	dropped	Number of packets in the egress queue that are dropped.
Policer	Inprofile	Number of in-profile packets for each policer.
	Outofprofile	Number of out-of-profile packets for each policer.

Related Commands

Command	Description
mls qos queue-set output buffers, on page 62	Allocates buffers to a queue set.

Command	Description
mls qos queue-set output threshold, on page 64	Configures the weighted tail-drop (WTD) thresholds, guarantees the availability of buffers, and configures the maximum memory allocation to a queue set.
mls qos srr-queue output cos-map, on page 69	Maps CoS values to an egress queue or maps CoS values to a queue and to a threshold ID.
mls qos srr-queue output dscp-map, on page 71	Maps DSCP values to an egress queue or maps DSCP values to a queue and to a threshold ID.
policy map, on page 80	Creates or modifies a policy map.
priority-queue	Enables the egress expedite queue on a port.
queue-set, on page 82	Maps a port to a queue set.
srr-queue bandwidth limit, on page 100	Limits the maximum output on a port.
srr-queue bandwidth shape, on page 102	Assigns the shaped weights and enables bandwidth shaping on the four egress queues mapped to a port.
srr-queue bandwidth share, on page 104	Assigns the shared weights and enables bandwidth sharing on the four egress queues mapped to a port.

show mls qos maps

To display quality of service (QoS) mapping information, use the **show mls qos maps** command in EXEC mode.

show mls qos maps [**cos-dscp**| **cos-output-q**| **dscp-cos**| **dscp-mutation** *dscp-mutation-name*| **dscp-output-q**| **ip-prec-dscp**| **policed-dscp**]

Syntax Description

cos-dscp	(Optional) Displays class of service (CoS)-to-DSCP map.
cos-output-q	(Optional) Displays the CoS output queue threshold map.
dscp-cos	(Optional) Displays DSCP-to-CoS map.
dscp-mutation *dscp-mutation-name*	(Optional) Displays the specified DSCP-to-DSCP-mutation map.
dscp-output-q	(Optional) Displays the DSCP output queue threshold map.
ip-prec-dscp	(Optional) Displays the IP-precedence-to-DSCP map.
policed-dscp	(Optional) Displays the policed-DSCP map.

Command Default

None

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS 15.0(2)EX	This command was introduced.

Usage Guidelines

During classification, QoS uses the mapping tables to represent the priority of the traffic and to derive a corresponding class of service (CoS) or Differentiated Services Code Point (DSCP) value from the received CoS, DSCP, or IP precedence value.

The policed-DSCP, DSCP-to-CoS, and the DSCP-to-DSCP-mutation maps appear as a matrix. The d1 column specifies the most-significant digit in the DSCP. The d2 row specifies the least-significant digit in the DSCP. The intersection of the d1 and d2 values provides the policed-DSCP, the CoS, or the mutated-DSCP value. For example, in the DSCP-to-CoS map, a DSCP value of 43 corresponds to a CoS value of 5.

The DSCP output queue threshold maps appear as a matrix. The d1 column specifies the most-significant digit of the DSCP number. The d2 row specifies the least-significant digit in the DSCP number. The intersection

of the d1 and the d2 values provides the queue ID and threshold ID. For example, in the DSCP output queue threshold map, a DSCP value of 43 corresponds to queue 1 and threshold 3 (01-03).

The CoS output queue threshold maps show the CoS value in the top row and the corresponding queue ID and threshold ID in the second row. For example, in the CoS output queue threshold map, a CoS value of 5 corresponds to queue 1 and threshold 3 (1-3).

Examples

This is an example of output from the **show mls qos maps** command:

```
Switch# show mls qos maps
   Policed-dscp map:
     d1 :  d2 0  1  2  3  4  5  6  7  8  9
     ----------------------------------------
      0 :    00 01 02 03 04 05 06 07 08 09
      1 :    10 11 12 13 14 15 16 17 18 19
      2 :    20 21 22 23 24 25 26 27 28 29
      3 :    30 31 32 33 34 35 36 37 38 39
      4 :    40 41 42 43 44 45 46 47 48 49
      5 :    50 51 52 53 54 55 56 57 58 59
      6 :    60 61 62 63

   Dscp-cos map:
     d1 :  d2 0  1  2  3  4  5  6  7  8  9
     ----------------------------------------
      0 :    00 00 00 00 00 00 00 00 01 01
      1 :    01 01 01 01 01 01 02 02 02 02
      2 :    02 02 02 02 03 03 03 03 03 03
      3 :    03 03 04 04 04 04 04 04 04 04
      4 :    05 05 05 05 05 05 05 05 06 06
      5 :    06 06 06 06 06 06 07 07 07 07
      6 :    07 07 07 07

   Cos-dscp map:
        cos:   0  1  2  3  4  5  6  7
     ---------------------------------
       dscp:   0  8 16 24 32 46 48 56

   IpPrecedence-dscp map:
     ipprec:   0  1  2  3  4  5  6  7
     ---------------------------------
       dscp:   0  8 16 24 32 40 48 56

   Dscp-outputq-threshold map:
     d1 :d2    0     1     2     3     4     5     6     7     8     9
     ------------------------------------------------------------
      0 :    03-03 03-03 03-03 03-03 03-03 03-03 03-03 03-03 04-01 04-01
      1 :    04-02 04-01 04-02 04-01 04-02 04-01 02-01 02-01 02-01 02-01
      2 :    02-01 02-01 02-01 02-01 02-02 03-01 02-01 02-01 02-01 02-01
      3 :    02-01 02-01 01-03 01-03 02-01 02-01 02-01 02-01 02-01 02-01
      4 :    01-03 01-03 01-03 01-03 01-03 01-03 01-03 01-03 02-03 02-03
      5 :    02-03 02-03 02-03 02-03 02-03 02-03 02-03 02-03 02-03 02-03
      6 :    02-03 02-03 02-03 02-03

   Cos-outputq-threshold map:
              cos:  0   1   2   3   4   5   6   7
              ------------------------------------
  queue-threshold: 3-3 4-3 2-1 2-2 1-3 1-3 2-3 2-3


   Dscp-dscp mutation map:
   Default DSCP Mutation Map:
     d1 :  d2 0  1  2  3  4  5  6  7  8  9
     ----------------------------------------
      0 :    00 01 02 03 04 05 06 07 08 09
      1 :    10 11 12 13 14 15 16 17 18 19
      2 :    20 21 22 23 24 25 26 27 28 29
      3 :    30 31 32 33 34 35 36 37 38 39
      4 :    40 41 42 43 44 45 46 47 48 49
      5 :    50 51 52 53 54 55 56 57 58 59
```

```
6 :    60 61 62 63
```

Related Commands

Command	Description
mls qos map, on page 58	Defines the CoS-to-DSCP map, DSCP-to-CoS map, DSCP-to-DSCP-mutation map, IP-precedence-to-DSCP map, and the policed-DSCP map.
mls qos srr-queue output cos-map, on page 69	Maps CoS values to an egress queue or maps CoS values to a queue and to a threshold ID.
mls qos srr-queue output dscp-map, on page 71	Maps DSCP values to an egress queue or maps DSCP values to a queue and to a threshold ID.

show mls qos queue-set

To display quality of service (QoS) settings for the egress queues, use the **show mls qos queue-set** command in EXEC mode.

show mls qos queue-set [*gset-id*]

Syntax Description

qset-id	(Optional) 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 Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS 15.0(2)EX	This command was introduced.

Examples

This is an example of output from the **show mls qos queue-set** command:

```
Switch# show mls qos queue-set
Queueset: 1
Queue    :        1       2       3       4
----------------------------------------------
buffers  :       25      25      25      25
threshold1:      100     200     100     100
threshold2:      100     200     100     100
reserved :       50      50      50      50
maximum  :       400     400     400     400
Queueset: 2
Queue    :        1       2       3       4
----------------------------------------------
buffers  :       25      25      25      25
threshold1:      100     200     100     100
threshold2:      100     200     100     100
reserved :       50      50      50      50
maximum  :       400     400     400     400
```

Related Commands

Command	Description
mls qos queue-set output buffers, on page 62	Allocates buffers to the queue set.
mls qos queue-set output threshold, on page 64	Configures the WTD thresholds, guarantees the availability of buffers, and configures the maximum memory allocation of the queue set.

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*]

Syntax Description

policy-map-name	(Optional) The policy map name.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS 15.0(2)EX	This command was introduced.

Usage Guidelines

Policy maps can include policers that specify the bandwidth limitations and the action to take if the limits are exceeded.

Note Though visible in the command-line help string, the **session**,**type**,**control-plane**, and **interface** keywords are not supported; statistics shown in the display should be ignored.

Examples

This is an example of output from the **show policy-map** command:

```
Switch# show policy-map
Policy Map videowizard_policy2
  class  videowizard_10-10-10-10
   set dscp 34
   police 100000000 2000000 exceed-action drop

 Policy Map mypolicy
  class  dscp5
   set dscp 6
```

Related Commands

Command	Description
policy map, on page 80	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.

srr-queue bandwidth limit

To limit the maximum output on a port, use the **srr-queue bandwidth limit** command in interface configuration mode. Use the **no** form of this command to return to the default setting.

srr-queue bandwidth limit *weight1*

no srr-queue bandwidth limit

Syntax Description

weight1	The port speed limit in percentage terms. The range is 10 to 90.

Command Default

The port is not rate limited and is set to 100 percent.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS 15.0(2)EX	This command was introduced.

Usage Guidelines

If you configure this command to 80 percent, the port is idle 20 percent of the time. The line rate drops to 80 percent of the connected speed. These values are not exact because the hardware adjusts the line rate in increments of six.

Examples

This example shows how to limit a port to 800 Mb/s:

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# srr-queue bandwidth limit 80
```

You can verify your settings by entering the **show mls qos interface** [*interface-id*] **queueing** privileged EXEC command.

Related Commands

Command	Description
mls qos queue-set output buffers, on page 62	Allocates buffers to the queue set.
mls qos srr-queue input cos-map	Maps CoS values to egress queue or maps CoS values to a queue and to a threshold ID.
mls qos srr-queue output dscp-map, on page 71	Maps DSCP values to an egress queue or maps DSCP values to a queue and to a threshold ID.

Command	Description
mls qos queue-set output threshold, on page 64	Configures the WTD thresholds, guarantees the availability of buffers, and configures the maximum memory allocation for the queue set.
queue-set, on page 82	Maps a port to a queue set.
show mls qos interface, on page 91	Displays QoS information.
srr-queue bandwidth shape, on page 102	Assigns the shaped weights and enables bandwidth shaping on the four egress queues mapped to a port.
srr-queue bandwidth share, on page 104	Assigns the shared weights and enables bandwidth sharing on the four egress queues mapped to a port.

srr-queue bandwidth shape

To assign the shaped weights and to enable bandwidth shaping on the four egress queues mapped to a port, use the **srr-queue bandwidth shape** command in interface configuration mode. Use the **no** form of this command to return to the default setting.

srr-queue bandwidth shape *weight1 weight2 weight3 weight4*

no srr-queue bandwidth shape

Syntax Description

weight1 weight2 weight3 weight4	The weights that specify the percentage of the port that is shaped. The inverse ratio (1/*weight*) specifies the shaping bandwidth for this queue. Separate each value with a space. The range is 0 to 65535.

Command Default

Weight1 is set to 25; weight2, weight3, and weight4 are set to 0, and these queues are in shared mode.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS 15.0(2)EX	This command was introduced.

Usage Guidelines

In shaped mode, the queues are guaranteed a percentage of the bandwidth, and they are rate-limited to that amount. Shaped traffic does not use more than the allocated bandwidth even if the link is idle. Use shaping to smooth bursty traffic or to provide a smoother output over time.

The shaped mode overrides the shared mode.

If you configure a shaped queue weight to 0 by using the **srr-queue bandwidth shape** interface configuration command, this queue participates in shared mode. The weight specified with the **srr-queue bandwidth shape** command is ignored, and the weights specified with the **srr-queue bandwidth share** interface configuration command for a queue come into effect.

When configuring queues for the same port for both shaping and sharing, make sure that you configure the lowest numbered queue for shaping.

Note The egress queue default settings are suitable for most situations. You should change them only when you have a thorough understanding of the egress queues and if these settings do not meet your QoS solution.

Examples

This example shows how to configure the queues for the same port for both shaping and sharing. Queues 2, 3, and 4 operate in the shared mode, because the weight ratios for these queues are set to 0. The bandwidth weight for queue 1 is 1/8, which is 12.5 percent. Queue 1 is guaranteed this bandwidth and limited to it; it does not extend its slot to the other queues even if the other queues have no traffic and are idle. Queues 2, 3, and 4 are in shared mode, and the setting for queue 1 is ignored. The bandwidth ratio allocated for the queues in shared mode is 4/(4+4+4), which is 33 percent:

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# srr-queue bandwidth shape 8 0 0 0
Switch(config-if)# srr-queue bandwidth share 4 4 4 4
```

You can verify your settings by entering the **show mls qos interface** [*interface-id*] **queueing** privileged EXEC command.

Related Commands

Command	Description
mls qos queue-set output buffers, on page 62	Allocates buffers to a queue set.
mls qos srr-queue input cos-map	Maps CoS values to an egress queue or maps CoS values to a queue and to a threshold ID.
mls qos srr-queue output dscp-map, on page 71	Maps DSCP values to an egress queue or maps DSCP values to a queue and to a threshold ID.
mls qos queue-set output threshold, on page 64	Configures the WTD thresholds, guarantees the availability of buffers, and configures the maximum memory allocation to a queue set.
priority-queue	Enables the egress expedite queue on a port.
queue-set, on page 82	Maps a port to a queue set.
show mls qos interface, on page 91	Displays QoS information.
srr-queue bandwidth share, on page 104	Assigns the shared weights and enables bandwidth sharing on the four egress queues mapped to a port.

srr-queue bandwidth share

To assign the shared weights and to enable bandwidth sharing on the four egress queues mapped to a port, use the **srr-queue bandwidth share** command in interface configuration mode. Use the **no** form of this command to return to the default setting.

srr-queue bandwidth share *weight1 weight2 weight3 weight4*

no srr-queue bandwidth share

Syntax Description

weight1 weight2 weight3 weight4	The ratios of *weight1*, *weight2*, *weight3*, and *weight4* specify the ratio of the frequency in which the SRR scheduler dequeues packets. Separate each value with a space. The range is 1 to 255.

Command Default

Equal bandwidth is allocated to each queue (Equal bandwidth for weight1, weight2, weight3, and weight4).

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS 15.0(2)EX	This command was introduced.

Usage Guidelines

The ratio of the weights is the ratio of frequency in which the shaped round-robin (SRR) scheduler dequeues packets from each queue.

The absolute value of each weight is meaningless, and only the ratio of parameters is used.

In shared mode, the queues share the bandwidth among them according to the configured weights. The bandwidth is guaranteed at this level but not limited to it. For example, if a queue empties and does not require a share of the link, the remaining queues can expand into the unused bandwidth and share it among themselves.

If you configure a shaped queue weight to 0 by using the **srr-queue bandwidth shape** interface configuration command, this queue participates in SRR shared mode. The weight specified with the **srr-queue bandwidth shape** command is ignored, and the weights specified with the **srr-queue bandwidth share** interface configuration command for a queue take effect.

When configuring queues for the same port for both shaping and sharing, make sure that you configure the lowest numbered queue for shaping.

Note The egress queue default settings are suitable for most situations. Change them only when you have a thorough understanding of the egress queues and if these settings do not meet your QoS solution.

Examples

This example shows how to configure the weight ratio of the SRR scheduler running on an egress port. Four queues are used. The bandwidth ratio allocated for each queue in shared mode is 1/(1+2+3+4), 2/(1+2+3+4), 3/(1+2+3+4), and 4/(1+2+3+4), which is 10 percent, 20 percent, 30 percent, and 40 percent for queues 1, 2, 3, and 4. This means that queue 4 has four times the bandwidth of queue 1, twice the bandwidth of queue 2, and one-and-a-third times the bandwidth of queue 3.

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# srr-queue bandwidth share 1 2 3 4
```

You can verify your settings by entering the **show mls qos interface** [*interface-id* **queueing**] privileged EXEC command.

Related Commands

Command	Description
mls qos queue-set output buffers, on page 62	Allocates buffers to a queue set.
mls qos queue-set output threshold, on page 64	Configures the weighted tail-drop (WTD) thresholds, guarantees the availability of buffers, and configures the maximum memory allocation to a queue set.
mls qos srr-queue input cos-map	Maps class of service (CoS) values to an egress queue or maps CoS values to a queue and to a threshold ID.
mls qos srr-queue output dscp-map, on page 71	Maps Differentiated Services Code Point (DSCP) values to an egress queue or maps DSCP values to a queue and to a threshold ID.
priority-queue	Enables the egress expedite queue on a port.
queue-set, on page 82	Maps a port to a queue set.
show mls qos interface, on page 91	Displays quality of service (QoS) information.
srr-queue bandwidth shape, on page 102	Assigns the shaped weights and enables bandwidth shaping on the four egress queues mapped to a port.

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
Cisco IOS 15.0(2)EX	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 a default class:

```
Switch(config)# policy-map policy1
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# trust dscp
Switch(config-pmap-c)# police 1000000 20000 exceed-action policed-dscp-transmit
Switch(config-pmap-c)# exit
```

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

Related Commands

Command	Description
class, on page 41	Defines a traffic classification match criteria (through the **police**, **set**, and **trust** policy-map class configuration command) for the specified class-map name.
police, on page 76	Defines a policer for classified traffic.
policy map, on page 80	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
set, on page 86	Classifies IP traffic by setting a DSCP or IP-precedence value in the packet.
show policy-map, on page 99	Displays QoS policy maps.

INDEX