



## **QoS Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)**

**First Published:** January 29, 2013

**Last Modified:** October 07, 2013

### **Americas Headquarters**

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

Text Part Number: OL-26763-02





## CONTENTS

5

---

### Preface

#### Preface vii

Document Conventions vii

Related Documentation ix

Obtaining Documentation and Submitting a Service Request ix

---

### CHAPTER 1

#### Using the Command-Line Interface 1

Information About Using the Command-Line Interface 1

Command Modes 1

Using the Help System 3

Understanding Abbreviated Commands 4

No and Default Forms of Commands 4

CLI Error Messages 4

Configuration Logging 5

How to Use the CLI to Configure Features 5

Configuring the Command History 5

Changing the Command History Buffer Size 6

Recalling Commands 6

Disabling the Command History Feature 7

Enabling and Disabling Editing Features 7

Editing Commands Through Keystrokes 8

Editing Command Lines That Wrap 9

Searching and Filtering Output of show and more Commands 10

Accessing the CLI on a Switch Stack 11

Accessing the CLI Through a Console Connection or Through Telnet 11

---

### CHAPTER 2

#### QoS Commands 13

class	14
class-map	16
match (class-map configuration)	17
match non-client-nrt	20
match wlan user-priority	21
policy-map	21
priority	24
queue-buffers ratio	25
queue-limit	27
qos wireless-default untrust	28
service-policy (Wired)	29
service-policy (WLAN)	31
set	32
show ap name service-policy	38
show ap name dot11	39
show class-map	42
show wireless client calls	42
show wireless client dot11	43
show wireless client mac-address (Call Control)	44
show wireless client mac-address (TCLAS)	45
show wireless client voice diagnostics	45
show policy-map	46
show wlan	50
trust device	52

---

**CHAPTER 3****Auto QoS Command Reference 55**

auto qos classify	55
auto qos trust	60
auto qos video	67
auto qos voip	77
show auto qos	89



---

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <http://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)





## Preface

- [Document Conventions](#), page vii
- [Related Documentation](#), page ix
- [Obtaining Documentation and Submitting a Service Request](#), page ix

## Document Conventions

This document uses the following conventions:

Convention	Description
^ or Ctrl	Both the ^ symbol and Ctrl represent the Control (Ctrl) key on a keyboard. For example, the key combination <b>^D</b> or <b>Ctrl-D</b> 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.)
<b>bold font</b>	Commands and keywords and user-entered text appear in <b>bold font</b> .
<i>Italic font</i>	Document titles, new or emphasized terms, and arguments for which you supply values are in <i>italic font</i> .
Courier font	Terminal sessions and information the system displays appear in <i>courier font</i> .
<b>Bold Courier font</b>	<b>Bold Courier font</b> indicates text that the user must enter.
[x]	Elements in square brackets are optional.
...	An ellipsis (three consecutive nonbolded periods without spaces) after a syntax element indicates that the element can be repeated.
	A vertical line, called a pipe, indicates a choice within a set of keywords or arguments.
[x   y]	Optional alternative keywords are grouped in brackets and separated by vertical bars.

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

### Reader Alert Conventions

This document may use the following conventions for reader alerts:



#### Note

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



#### Tip

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



#### Caution

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



#### Timesaver

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



#### Warning

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



## Related Documentation

**Note**

---

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

---

- Cisco Catalyst 3850 Switch documentation, located at:  
[http://www.cisco.com/go/cat3850\\_docs](http://www.cisco.com/go/cat3850_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](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>
- Error Message Decoder, located at:  
<https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi>

## Obtaining Documentation and Submitting a Service Request

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

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

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





# Using the Command-Line Interface

- [Information About Using the Command-Line Interface, page 1](#)
- [How to Use the CLI to Configure Features, page 5](#)

## Information About Using the Command-Line Interface

### Command Modes

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

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

When you start a session, you begin in user mode, often called user EXEC mode. Only a limited subset of the commands are available in user EXEC mode. For example, most of the user EXEC commands are one-time commands, such as **show** commands, which show the current configuration status, and **clear** commands, which clear counters or interfaces. The user EXEC commands are not saved when the 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 <b>logout</b> or <b>quit</b> .	Use this mode to <ul style="list-style-type: none"> <li>• Change terminal settings.</li> <li>• Perform basic tests.</li> <li>• Display system information.</li> </ul>
Privileged EXEC	While in user EXEC mode, enter the <b>enable</b> command.	Switch#	Enter <b>disable</b> 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 <b>configure</b> command.	Switch(config)#	To exit to privileged EXEC mode, enter <b>exit</b> or <b>end</b> , or press <b>Ctrl-Z</b> .	Use this mode to configure parameters that apply to the entire switch.
VLAN configuration	While in global configuration mode, enter the <b>vlan</b> <i>vlan-id</i> command.	Switch(config-vlan)#	To exit to global configuration mode, enter the <b>exit</b> command. To return to privileged EXEC mode, press <b>Ctrl-Z</b> or enter <b>end</b> .	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 <b>interface</b> command (with a specific interface).	Switch(config-if)#	To exit to global configuration mode, enter <b>exit</b> . To return to privileged EXEC mode, press <b>Ctrl-Z</b> or enter <b>end</b> .	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 <b>line vty</b> or <b>line console</b> command.	Switch(config-line)#	To exit to global configuration mode, enter <b>exit</b> .  To return to privileged EXEC mode, press <b>Ctrl-Z</b> or enter <b>end</b> .	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
<b>Step 1</b>	<b>help</b>  <b>Example:</b> Switch# <b>help</b>	Obtains a brief description of the help system in any command mode.
<b>Step 2</b>	<i>abbreviated-command-entry ?</i>  <b>Example:</b> Switch# <b>di?</b> dir disable disconnect	Obtains a list of commands that begin with a particular character string.
<b>Step 3</b>	<i>abbreviated-command-entry &lt;Tab&gt;</i>  <b>Example:</b> Switch# <b>sh conf&lt;tab&gt;</b> Switch# <b>show configuration</b>	Completes a partial command name.

	Command or Action	Purpose
Step 4	?  Example: Switch> ?	Lists all commands available for a particular command mode.
Step 5	<i>command</i> ?  Example: Switch> <b>show</b> ?	Lists the associated keywords for a command.
Step 6	<i>command keyword</i> ?  Example: Switch(config)# <b>cdp holdtime</b> ? <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 (?) without any space between the command and the question mark.  The possible keywords that you can enter with the command appear.
% Incomplete command.	You did not enter all of the keywords or values required by this command.	Reenter the command followed by a question mark (?) with a space between the command and the question mark.  The possible keywords that you can enter with the command appear.
% Invalid input detected at '^' marker.	You entered the command incorrectly. The caret (^) marks the point of the error.	Enter a question mark (?) to display all of the commands that are available in this command mode.  The possible keywords that you can enter with the command appear.

## Configuration Logging

You can log and view changes to the 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
<b>Step 1</b>	<b>terminal history</b> [ <i>size number-of-lines</i> ]  <b>Example:</b> Switch# <b>terminal history size 200</b>	Changes the number of command lines that the switch records during the current terminal session in privileged EXEC mode. You can configure the size from 0 to 256.

## Recalling Commands

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



### Note

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

### SUMMARY STEPS

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

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>Ctrl-P</b> or use the <b>up arrow</b> key	Recalls commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.
<b>Step 2</b>	<b>Ctrl-N</b> or use the <b>down arrow</b> key	Returns to more recent commands in the history buffer after recalling commands with <b>Ctrl-P</b> or the up arrow key. Repeat the key sequence to recall successively more recent commands.



	Command or Action	Purpose
<b>Step 3</b>	<b>show history</b>  <b>Example:</b> Switch# <code>show history</code>	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 <b>terminal history</b> global configuration command and the <b>history</b> 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
<b>Step 1</b>	<b>terminal no history</b>  <b>Example:</b> Switch# <code>terminal no history</code>	Disables the feature during the current terminal session in privileged EXEC mode.

## Enabling and Disabling Editing Features

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

### SUMMARY STEPS

1. `terminal editing`
2. `terminal no editing`

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>terminal editing</b>  <b>Example:</b> Switch# <code>terminal editing</code>	Reenables the enhanced editing mode for the current terminal session in privileged EXEC mode.

	Command or Action	Purpose
Step 2	<b>terminal no editing</b>  <b>Example:</b> Switch# <code>terminal no editing</code>	Disables the enhanced editing mode for the current terminal session in privileged EXEC mode.

## Editing Commands Through Keystrokes

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



### Note

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

**Table 3: Editing Commands**

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

<b>Esc D</b>	Deletes from the cursor to the end of the word.
<b>Esc C</b>	Capitalizes at the cursor.
<b>Esc L</b>	Changes the word at the cursor to lowercase.
<b>Esc U</b>	Capitalizes letters from the cursor to the end of the word.
<b>Ctrl-V</b> or <b>Esc Q</b>	Designates a particular keystroke as an executable command, perhaps as a shortcut.
<b>Return</b> key	Scrolls down a line or screen on displays that are longer than the terminal screen can display.  <b>Note</b> The More prompt is used for any output that has more lines than can be displayed on the terminal screen, including <b>show</b> command output. You can use the <b>Return</b> and <b>Space</b> bar keystrokes whenever you see the More prompt.
<b>Space</b> bar	Scrolls down one screen.
<b>Ctrl-L</b> or <b>Ctrl-R</b>	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 extends beyond a single line on the screen.

## SUMMARY STEPS

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

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>access-list</b>  <b>Example:</b> <pre>Switch(config)# access-list 101 permit tcp 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</pre>	<p>Displays the global configuration command entry that extends beyond one line.</p> <p>When the cursor first reaches the end of the line, the line is shifted ten spaces to the left and redisplayed. The dollar sign (\$) shows that the line has been scrolled to the left. Each time the cursor reaches the end of the line, the line is again shifted ten spaces to the left.</p>
<b>Step 2</b>	<b>Ctrl-A</b>  <b>Example:</b> <pre>Switch(config)# access-list 101 permit tcp 10.15.22.25 255.255.255.0 10.15.25\$</pre>	<p>Checks the complete syntax.</p> <p>The dollar sign (\$) appears at the end of the line to show that the line has been scrolled to the right.</p>
<b>Step 3</b>	<b>Return key</b>	<p>Execute the commands.</p> <p>The software assumes that you have a terminal screen that is 80 columns wide. If you have a different width, use the <b>terminal width</b> privileged EXEC command to set the width of your terminal.</p> <p>Use line wrapping with the command history feature to recall and modify previous complex command entries.</p>

## 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
<b>Step 1</b>	<code>{show   more} command   {begin   include   exclude} regular-expression</code>	Searches and filters the output.

	Command or Action	Purpose
	<p><b>Example:</b></p> <pre>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</pre>	<p>Expressions are case sensitive. For example, if you enter   <b>exclude output</b>, the lines that contain <b>output</b> are not displayed, but the lines that contain <b>output</b> appear.</p>

## Accessing the CLI on a Switch Stack

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

You manage the switch stack and the stack member interfaces through the active switchstack master. You cannot manage stack members on an individual switch basis. You can connect to the active switchstack master through the console port or the Ethernet management port of one or more stack members. Be careful with using multiple CLI sessions on the active switchstack master. Commands that you enter in one session are not displayed in the other sessions. Therefore, it is possible to lose track of the session from which you entered commands.



### Note

We recommend using one CLI session when managing the switch stack.

If you want to configure a specific stack member port, you must include the stack member number in the CLI command interface notation.

To debug the standby switch, use the **session standby ios** privileged EXEC command from the active switch to access the IOS console of the standby switch. To debug a specific stack member, use the **session switch stack-member-number** privileged EXEC command from the active switch to access the diagnostic shell of the stack member. For more information about these commands, see the switch command reference.

## 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.



## QoS Commands

---

- [class](#), page 14
- [class-map](#), page 16
- [match \(class-map configuration\)](#), page 17
- [match non-client-nrt](#), page 20
- [match wlan user-priority](#), page 21
- [policy-map](#), page 21
- [priority](#), page 24
- [queue-buffers ratio](#), page 25
- [queue-limit](#), page 27
- [qos wireless-default untrust](#), page 28
- [service-policy \(Wired\)](#), page 29
- [service-policy \(WLAN\)](#), page 31
- [set](#), page 32
- [show ap name service-policy](#), page 38
- [show ap name dot11](#), page 39
- [show class-map](#), page 42
- [show wireless client calls](#), page 42
- [show wireless client dot11](#), page 43
- [show wireless client mac-address \(Call Control\)](#), page 44
- [show wireless client mac-address \(TCLAS\)](#), page 45
- [show wireless client voice diagnostics](#), page 45
- [show policy-map](#), page 46
- [show wlan](#), page 50
- [trust device](#), page 52

# 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

<i>class-map-name</i>	The class map name.
<b>class-default</b>	Refers to a system default class that matches unclassified packets.

## Command Default

No policy map class-maps are defined.

## Command Modes

Policy-map configuration

## Command History

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

## Usage Guidelines

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

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

- **admit**—Admits a request for Call Admission Control (CAC)
- **bandwidth**—Specifies the bandwidth allocated to the class.
- **exit**—Exits the policy-map class configuration mode and returns to policy-map configuration mode.
- **no**—Returns a command to its default setting.
- **police**—Defines a policer or aggregate policer for the classified traffic. The policer specifies the bandwidth limitations and the action to take when the limits are exceeded. For more information about this command, see *Cisco IOS Quality of Service Solutions Command Reference* available on Cisco.com.
- **priority**—Assigns scheduling priority to a class of traffic belonging to a policy map.
- **queue-buffers**—Configures the queue buffer for the class.



- **queue-limit**—Specifies the maximum number of packets the queue can hold for a class policy configured in a policy map.
- **service-policy**—Configures a QoS service policy.
- **set**—Specifies a value to be assigned to the classified traffic. For more information, see [set](#), on page 32
- **shape**—Specifies average or peak rate traffic shaping. For more information about this command, see *Cisco IOS Quality of Service Solutions Command Reference* available on Cisco.com.

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

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

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

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

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

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

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

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

Switch(config)# class-map cm-4
Switch(config-cmap)# match ip dscp 40
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)# set precedence 5
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit

Switch# show policy-map pm3
Policy Map pm3
  Class cm-3
```

```

    set dscp 4
Class cm-4
    set precedence 5
Class class-default
    set dscp af11

```

### Related Topics

- [class-map, on page 16](#)
- [policy-map, on page 21](#)
- [show policy-map, on page 46](#)
- [set, on page 32](#)

## 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

<b>match-any</b>	(Optional) Perform a logical-OR of the matching statements under this class map. One or more criteria must be matched.
<b>type</b>	(Optional) Configures the CPL class map.
<i>class-map-name</i>	The class map name.

### Command Default

No class maps are defined.

### Command Modes

Global configuration  
Policy map configuration

### Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.
Cisco IOS XE 3.3SE	The <b>type</b> keyword was added.

**Usage Guidelines**

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

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

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

- **description**—Describes the class map (up to 200 characters). The **show class-map** privileged EXEC command displays the description and the name of the class map.
- **exit**—Exits from QoS class-map configuration mode.
- **match**—Configures classification criteria.
- **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.

The ACL can have multiple access control entries (ACEs).

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 Topics**

[policy-map, on page 21](#)

[show policy-map, on page 46](#)

## 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 {nameacl-name | acl-index} | class-map class-map-name | cos cos-value | dscp dscp-value | [ip | dscp dscp-list | [ip] precedence ip-precedence-list] precedence precedence-value1...value4 | qos-group qos-group-value | vlan vlan-id}
```

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

**Syntax Description**

<b>access-group</b>	Specifies an access group.
<b>name</b> <i>acl-name</i>	Specifies the name of an IP standard or extended access control list (ACL) or MAC ACL.
<i>acl-index</i>	Specifies the number of an IP standard or extended access control list (ACL) or MAC ACL. For an IP standard ACL, the ACL index range is 1 to 99 and 1300 to 1999. For an IP extended ACL, the ACL index range is 100 to 199 and 2000 to 2699.
<b>class-map</b> <i>class-map-name</i>	Uses a traffic class as a classification policy and specifies a traffic class name to use as the match criterion.
<b>cos</b> <i>cos-value</i>	Matches a packet on the basis of a Layer 2 class of service (CoS)/Inter-Switch Link (ISL) marking. The cos-value is from 0 to 7. You can specify up to four CoS values in one <b>match cos</b> statement, separated by a space.
<b>dscp</b> <i>dscp-value</i>	Specifies the parameters for each DSCP value. You can specify a value in the range 0 to 63 specifying the differentiated services code point value.
<b>ip dscp</b> <i>dscp-list</i>	Specifies a list of up to eight IP Differentiated Services Code Point (DSCP) values to match against incoming packets. Separate each value with a space. The range is 0 to 63. You also can enter a mnemonic name for a commonly used value.
<b>ip precedence</b> <i>ip-precedence-list</i>	Specifies a list of up to eight IP-precedence values to match against incoming packets. Separate each value with a space. The range is 0 to 7. You also can enter a mnemonic name for a commonly used value.
<b>precedence</b> <i>precedence-value1...value4</i>	Assigns an IP precedence value to the classified traffic. The range is 0 to 7. You also can enter a mnemonic name for a commonly used value.
<b>qos-group</b> <i>qos-group-value</i>	Identifies a specific QoS group value as a match criterion. The range is 0 to 31.
<b>vlan</b> <i>vlan-id</i>	Identifies a specific VLAN as a match criterion. The range is 1 to 4095.

**Command Default**

No match criteria are defined.

**Command Modes**

Class-map configuration

**Command History**

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.
Cisco IOS XE 3.3SE	The <b>class-map</b> <i>class-map-name</i> , <b>cos</b> <i>cos-value</i> , <b>qos-group</b> <i>qos-group-value</i> , and <b>vlan</b> <i>vlan-id</i> keywords were added.

**Usage Guidelines**

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

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

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



**Note** The ACL must be an extended named ACL.

- **match ip dscp** *dscp-list*
- **match ip precedence** *ip-precedence-list*

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

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

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

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

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
```

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

```
Switch(config) # class-map match-any class4
Switch(config-cmap) # match cos 4
Switch(config-cmap) # exit
```

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

```
Switch(config) # class-map match-any class4
Switch(config-cmap) # match cos 4
Switch(config-cmap) # exit
```

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

## match non-client-nrt

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

**match non-client-nrt**

**no match non-client-nrt**

**Syntax Description** This command has no arguments or keywords.

**Command Default** None

**Command Modes** Class-map

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

**Usage Guidelines** None

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

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

## match wlan user-priority

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

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

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

### Syntax Description

*wlan-value*

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

### Command Default

None

### Command Modes

Class-map

### Command History

#### Release

#### Modification

Cisco IOS XE 3.2SE

This command was introduced.

### Usage Guidelines

None

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

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

## policy-map

To create or modify a policy map that can be attached to multiple physical ports or switch virtual interfaces (SVIs) and to enter policy-map configuration mode, use the **policy-map** command in global configuration mode. Use the **no** form of this command to delete an existing policy map and to return to global configuration mode.

**policy-map** *policy-map-name*

**no policy-map** *policy-map-name*

### Syntax Description

*policy-map-name*

Name of the policy map.

**Command Default** No policy maps are defined.

**Command Modes** Global configuration

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

**Usage Guidelines** After entering the **policy-map** command, you enter policy-map configuration mode, and these configuration commands are available:

- **class**—Defines the classification match criteria for the specified class map.
- **description**—Describes the policy map (up to 200 characters).
- **exit**—Exits policy-map configuration mode and returns you to global configuration mode.
- **no**—Removes a previously defined policy map.
- **sequence-interval**—Enables sequence number capability.

To return to global configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

Before configuring policies for classes whose match criteria are defined in a class map, use the **policy-map** command to specify the name of the policy map to be created, added to, or modified. Entering the **policy-map** command also enables the policy-map configuration mode in which you can configure or modify the class policies for that policy map.

You can configure class policies in a policy map only if the classes have match criteria defined for them. To configure the match criteria for a class, use the **class-map** global configuration and **match** class-map configuration commands. You define packet classification on a physical-port basis.

Only one policy map per ingress port is supported. You can apply the same policy map to multiple physical ports.

You can apply a nonhierarchical policy maps to physical ports. A nonhierarchical policy map is the same as the port-based policy maps in the switch.

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

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



**Note**

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

This example shows how to create a policy map called policy1. When attached to the ingress port, it matches all the incoming traffic defined in class1, sets the IP DSCP to 10, and polices the traffic at an average rate of 1 Mb/s and bursts at 20 KB. Traffic less than the profile is sent.

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

This example show you how to configure hierarchical polices:

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

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

Switch(config)# policy-map child
Switch(config-pmap)# class c1
Switch(config-pmap-c)# priority level 1
Switch(config-pmap-c)# police rate percent 20 conform-action transmit exceed action drop
Switch(config-pmap-c-police)# exit
Switch(config-pmap-c)# exit

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

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

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

This example shows how to delete a policy map:

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

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

**Related Topics**

[class](#), on page 14

[class-map](#), on page 16

[service-policy \(Wired\)](#), on page 29

[show policy-map](#), on page 46

# priority

To assign priority to a class of traffic belonging to a policy map, use the **priority** command in policy-map class configuration mode. To remove a previously specified priority for a class, use the **no** form of this command.

**priority** [*Kbps* [*burst -in-bytes*] ] | **level** *level-value* [*Kbps* [*burst -in-bytes*] ] | **percent** *percentage* [*Kb/s* [*burst -in-bytes*] ] ]

**no priority** [*Kb/s* [*burst -in-bytes*] ] | **level** *level value* [*Kb/s* [*burst -in-bytes*] ] | **percent** *percentage* [*Kb/s* [*burst -in-bytes*] ] ]

## Syntax Description

<i>Kb/s</i>	(Optional) Guaranteed allowed bandwidth, in kilobits per second (kbps), for the priority traffic. The amount of guaranteed bandwidth varies according to the interface and platform in use. Beyond the guaranteed bandwidth, the priority traffic will be dropped in the event of congestion to ensure that the nonpriority traffic is not starved. The value must be between 1 and 2,000,000 kbps.
<i>burst -in-bytes</i>	(Optional) Burst size in bytes. The burst size configures the network to accommodate temporary bursts of traffic. The default burst value, which is computed as 200 milliseconds of traffic at the configured bandwidth rate, is used when the burst argument is not specified. The range of the burst is from 32 to 2000000 bytes.
<b>level</b> <i>level-value</i>	(Optional) Assigns priority level. Available values for <i>level-value</i> are 1 and 2. Level 1 is a higher priority than Level 2. Level 1 reserves bandwidth and goes first, so latency is very low. Reserve the bandwidth even if you do not use it. Both levels 1 and 2 can reserve bandwidth.
<b>percent</b> <i>percentage</i>	(Optional) Specifies the amount of guaranteed bandwidth to be specified by the percent of available bandwidth.

## Command Default

No priority is set.

## Command Modes

Policy-map class configuration

## Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.
Cisco IOS XE 3.3SE	The <i>Kbps</i> , <i>burst -in-bytes</i> , and <b>percent percentage</b> keywords were added.

**Usage Guidelines**

This command configures low latency queuing (LLQ), providing strict priority queuing (PQ) for class-based weighted fair queuing (CBWFQ). Strict PQ allows delay-sensitive data such as voice to be dequeued and sent before packets in other queues are dequeued.

The priority command allows you to set up classes based on a variety of criteria (not just User Datagram Ports [UDP] ports) and assign priority to them, and is available for use on serial interfaces and ATM permanent virtual circuits (PVCs). A similar command, the **ip rtp priority** command, allows you to stipulate priority flows based only on UDP port numbers and is not available for ATM PVCs.

When the device is not congested, the priority class traffic is allowed to exceed its allocated bandwidth. When the device is congested, the priority class traffic above the allocated bandwidth is discarded.

The bandwidth and priority commands cannot be used in the same class, within the same policy map. However, these commands can be used together in the same policy map.

Within a policy map, you can give one or more classes priority status. When multiple classes within a single policy map are configured as priority classes, all traffic from these classes is queued to the same, single, priority queue.

When the policy map containing class policy configurations is attached to the interface to stipulate the service policy for that interface, available bandwidth is assessed. If a policy map cannot be attached to a particular interface because of insufficient interface bandwidth, the policy is removed from all interfaces to which it was successfully attached.

**Example**

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

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

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

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

Switch(config)#policy-map policy1
Switch(config-pmap)#class cm2
Switch(config-pmap-c)#priority level 2
Switch(config-pmap-c)#police 1m
```

## queue-buffers ratio

To configure the queue buffer for the class, use the **queue-buffers ratio** command in policy-map class configuration mode. Use the **no** form of this command to remove the ratio limit.

**queue-buffers ratio** *ratio limit*

**no queue-buffers ratio** *ratio limit*

<b>Syntax Description</b>	<i>ratio limit</i> (Optional) Configures the queue buffer for the class. Enter the queue buffers ratio limit (0-100).
---------------------------	---

**Command Default** No queue buffer for the class is defined.

**Command Modes** Policy-map class configuration

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE 3.2SE	This command was introduced.

**Usage Guidelines** Either the **bandwidth**, **shape**, or **priority** command must be used before using this command. For more information about these commands, see *Cisco IOS Quality of Service Solutions Command Reference* available on Cisco.com

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



**Note** The queue-buffer ratio is supported on both wired and wireless ports, but the queue-buffer ratio cannot be configured with a queue-limit.

### Example

The following example sets the queue buffers ratio to 10 percent:

```
Switch(config)# policy-map policy_queuebuf01
Switch(config-pmap)# class-map class_queuebuf01
Switch(config-cmap)# exit
Switch(config)# policy policy_queuebuf01
Switch(config-pmap)# class class_queuebuf01
Switch(config-pmap-c)# bandwidth percent 80
Switch(config-pmap-c)# queue-buffers ratio 10
Switch(config-pmap)# end
```

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

### Related Topics

[show policy-map, on page 46](#)

# queue-limit

To specify or modify the maximum number of packets the queue can hold for a class policy configured in a policy map, use the **queue-limit** policy-map class configuration command. To remove the queue packet limit from a class, use the **no** form of this command.

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

## Syntax Description

<i>queue-limit-size</i>	The maximum size of the queue. The maximum varies according to the optional unit of measure keyword specified ( bytes, ms, us, or packets).
<b>cos</b> <i>cos-value</i>	Specifies parameters for each cos value. CoS values are from 0 to 7.
<b>dscp</b> <i>dscp-value</i>	Specifies parameters for each DSCP value. You can specify a value in the range 0 to 63 specifying the differentiated services code point value for the type of queue limit .
<b>percent</b> <i>percentage-of-packets</i>	A percentage in the range 1 to 100 specifying the maximum percentage of packets that the queue for this class can accumulate.

## Command Default

None

## Command Modes

Policy-map class configuration

## Command History

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

## Usage Guidelines

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



### Note

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

Weighted fair queuing (WFQ) creates a queue for every class for which a class map is defined. Packets satisfying the match criteria for a class accumulate in the queue reserved for the class until they are sent, which occurs when the queue is serviced by the fair queuing process. When the maximum packet threshold you defined for the class is reached, queuing of any further packets to the class queue causes tail drop.

You use queue limits to configure Weighted Tail Drop (WTD). WTD ensures the configuration of more than one threshold per queue. Each class of service is dropped at a different threshold value to provide for QoS differentiation.

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

### Example

The following example configures a policy map called port-queue to contain policy for a class called dscp-1. The policy for this class is set so that the queue reserved for it has a maximum packet limit of 20 percent:

```
Switch(config)# policy-map policy11
Switch(config-pmap)# class dscp-1
Switch(config-pmap-c)# bandwidth percent 20
Switch(config-pmap-c)# queue-limit dscp 1 percent 20
```

## qos wireless-default untrust

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

**qos wireless-default-untrust**

**no qos wireless-default-untrust**

### Syntax Description

This command has no arguments or keywords.

### Command Default

By default, the wireless traffic is untrusted.

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

### Command Modes

Configuration

### Command History

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

**Usage Guidelines** 

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



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

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

**Example**

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

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

## service-policy (Wired)

To apply a policy map to a physical port or a switch virtual interface (SVI), use the **service-policy** command in interface configuration mode. Use the **no** form of this command to remove the policy map and port association.

**service-policy** {input | output} *policy-map-name*

**no service-policy** {input | output} *policy-map-name*

**Syntax Description**

**input** *policy-map-name* Apply the specified policy map to the input of a physical port or an SVI.

**output** *policy-map-name* Apply the specified policy map to the output of a physical port or an SVI.

**Command Default**

No policy maps are attached to the port.

**Command Modes** WLAN interface configuration

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

**Usage Guidelines** A policy map is defined by the **policy map** command.

Only one policy map is supported per port, per direction. In other words, only one input policy and one output policy is allowed on any one port.

You can apply a policy map to incoming traffic on a physical port or on an SVI. *QoS Configuration Guide (Catalyst 3850 Switches)*.



**Note** Though visible in the command-line help strings, the **history** keyword is not supported, and you should ignore the statistics that it gathers.

This example shows how to apply plcmap1 to an physical ingress port:

```
Switch(config)# interface gigabitEthernet2/0/1
Switch(config-if)# service-policy input plcmap1
```

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
```

The following example displays a VLAN policer configuration. At the end of this configuration, the VLAN policy map is applied to an interface for QoS:

```
Switch# configure terminal
Switch(config)# class-map vlan100
Switch(config-cmap)# match vlan 100
Switch(config-cmap)# exit
Switch(config)# policy-map vlan100
Switch(config-pmap)# policy-map class vlan100
Switch(config-pmap-c)# police 100000 bc conform-action transmit exceed-action drop
Switch(config-pmap-c-police)# end
Switch# configure terminal
Switch(config)# interface gigabitEthernet1/0/5
Switch(config-if)# service-policy input vlan100
```

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

### Related Topics

[policy-map](#), on page 21

[show policy-map](#), on page 46



## service-policy (WLAN)

To configure the WLAN quality of service (QoS) service policy, use the **service-policy** command. To disable a QoS policy on a WLAN, use the **no** form of this command.

**service-policy** [client] {input| output} *policy-name*

**no service-policy** [client] {input| output} *policy-name*

### Syntax Description

<b>client</b>	(Optional) Assigns a policy map to all clients in the WLAN.
<b>input</b>	Assigns an input policy map.
<b>output</b>	Assigns an output policy map.
<i>policy-name</i>	The policy name.

### Command Default

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

### Command Modes

WLAN configuration

### Command History

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

### Usage Guidelines

You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

This example shows how to configure the input QoS service policy on a WLAN:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# service-policy input policy-test
```

This example shows how to disable the input QoS service policy on a WLAN:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# no service-policy input policy-test
```

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

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# service-policy output platinum
```

## set

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

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

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

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

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

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

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

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

**qos-group***table-map-name*| **wlantable** *table-map-name*

---

**Syntax Description****cos**

Sets the Layer 2 class of service (CoS) value or user priority of an outgoing packet. You can specify these values:

- *cos-value*—CoS value from 0 to 7. You also can enter a mnemonic name for a commonly used value.
- Specify a packet-marking category to set the CoS value of the packet. If you also configure a table map for mapping and converting packet-marking values, this establishes the "map from" packet-marking category. Packet-marking category keywords:
  - **cos**—Sets a value from the CoS value or user priority.
  - **dscp**—Sets a value from packet differentiated services code point (DSCP).
  - **precedence**—Sets a value from packet precedence.
  - **qos-group**—Sets a value from the QoS group.
  - **wlan**—Sets the WLAN user priority values.
- (Optional) **table** *table-map-name*—Indicates that the values set in a specified table map are used to set the CoS value. Enter the name of the table map used to specify the CoS value. The table map name can be a maximum of 64 alphanumeric characters.

If you specify a packet-marking category but do not specify the table map, the default action is to copy the value associated with the packet-marking category as the CoS value. For example, if you enter the **set cos precedence** command, the precedence (packet-marking category) value is copied and used as the CoS value.

---

---

**dscp**

Sets the differentiated services code point (DSCP) value to mark IP(v4) and IPv6 packets. You can specify these values:

- *cos-value*—Number that sets the DSCP value. The range is from 0 to 63. You also can enter a mnemonic name for a commonly used value.
- Specify a packet-marking category to set the DSCP value of the packet. If you also configure a table map for mapping and converting packet-marking values, this establishes the "map from" packet-marking category. Packet-marking category keywords:
  - **cos**—Sets a value from the CoS value or user priority.
  - **dscp**—Sets a value from packet differentiated services code point (DSCP).
  - **precedence**—Sets a value from packet precedence.
  - **qos-group**—Sets a value from the QoS group.
  - **wlan**—Sets a value from WLAN.
- (Optional)**table** *table-map-name*—Indicates that the values set in a specified table map will be used to set the DSCP value. Enter the name of the table map used to specify the DSCP value. The table map name can be a maximum of 64 alphanumeric characters.
 

If you specify a packet-marking category but do not specify the table map, the default action is to copy the value associated with the packet-marking category as the DSCP value. For example, if you enter the **set dscp cos** command, the CoS value (packet-marking category) is copied and used as the DSCP value.

---

**ip**

Sets IP values to the classified traffic. You can specify these values:

- **dscp**—Specify an IP DSCP value from 0 to 63 or a packet marking category.
  - **precedence**—Specify a precedence-bit value in the IP header; valid values are from 0 to 7 or specify a packet marking category.
-

---

**precedence**

Sets the precedence value in the packet header. You can specify these values:

- *precedence-value*— Sets the precedence bit in the packet header; valid values are from 0 to 7. You also can enter a mnemonic name for a commonly used value.
- Specify a packet marking category to set the precedence value of the packet.
  - **cos**—Sets a value from the CoS or user priority.
  - **dscp**—Sets a value from packet differentiated services code point (DSCP).
  - **precedence**—Sets a value from packet precedence.
  - **qos-group**—Sets a value from the QoS group.
- (Optional) **table** *table-map-name*—Indicates that the values set in a specified table map will be used to set the precedence value. Enter the name of the table map used to specify the precedence value. The table map name can be a maximum of 64 alphanumeric characters.

If you specify a packet-marking category but do not specify the table map, the default action is to copy the value associated with the packet-marking category as the precedence value. For example, if you enter the **set precedence cos** command, the CoS value (packet-marking category) is copied and used as the precedence value.

---

---

**qos-group**

Assigns a QoS group identifier that can be used later to classify packets.

- *qos-group-value*—Sets a QoS value to the classified traffic. The range is 0 to 31. You also can enter a mnemonic name for a commonly used value.
- **dscp**—Sets the original DSCP field value of the packet as the QoS group value.
- **precedence**—Sets the original precedence field value of the packet as the QoS group value.
- (Optional)**table** *table-map-name*—Indicates that the values set in a specified table map will be used to set the DSCP or precedence value. Enter the name of the table map used to specify the value. The table map name can be a maximum of 64 alphanumeric characters.

If you specify a packet-marking category (**dscp** or **precedence**) but do not specify the table map, the default action is to copy the value associated with the packet-marking category as the QoS group value. For example, if you enter the **set qos-group precedence** command, the precedence value (packet-marking category) is copied and used as the QoS group value.

---

<b>wlan user-priority</b> <i>wlan-user-priority</i>	<p>Assigns a WLAN user-priority to the classified traffic. You can specify these values:</p> <ul style="list-style-type: none"> <li>• <i>wlan-user-priority</i>—Sets a WLAN user priority to the classified traffic. The range is 0 to 7.</li> <li>• <b>cos</b>—Sets the Layer 2 CoS field value as the WLAN user priority.</li> <li>• <b>dscp</b>—Sets the DSCP field value as the WLAN user priority.</li> <li>• <b>precedence</b>—Sets the precedence field value as the WLAN user priority.</li> <li>• <b>wlan</b>—Sets the WLAN user priority field value as the WLAN user priority.</li> <li>• (Optional)<b>table</b> <i>table-map-name</i>—Indicates that the values set in a specified table map will be used to set the WLAN user priority value. Enter the name of the table map used to specify the value. The table map name can be a maximum of 64 alphanumeric characters.</li> </ul> <p>If you specify a packet-marking category but do not specify the table map, the default action is to copy the value associated with the packet-marking category as the WLAN user priority. For example, if you enter the <b>set wlan user-priority cos</b> command, the cos value (packet-marking category) is copied and used as the WLAN user priority.</p>
---	---

**Command Default** No traffic classification is defined.

**Command Modes** Policy-map class configuration

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.
Cisco IOS XE 3.3SE	The <b>cos</b> , <b>dscp</b> , <b>qos-group</b> , <b>wlan</b> <b>table</b> <i>table-map-name</i> , keywords were added.

**Usage Guidelines** For the **set dscp** *dscp-value* command, the **set cos** *cos-value* command, and the **set ip precedence** *precedence-value* command, you can enter a mnemonic name for a commonly used value. For example, you

can enter the **set dscp af11** command, which is the same as entering the **set dscp 10** command. You can enter the **set ip precedence critical** command, which is the same as entering the **set ip precedence 5** command. For a list of supported mnemonics, enter the **set dscp ?** or the **set ip precedence ?** command to see the command-line help strings.

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

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

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

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

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

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 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 Topics

[class, on page 14](#)

[policy-map, on page 21](#)

[show policy-map, on page 46](#)

## show ap name service-policy

To display service-policy information for a specific Cisco lightweight access point, use the **show ap name service-policy** command.

**show ap name** *ap-name* **service-policy**

### Syntax Description

---

<i>ap-name</i>	Name of the Cisco lightweight access point.
----------------	---

---



**Command Default**

None

**Command Modes**

Any command mode

**Command History**

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

This example shows how to display service-policy information for a specific Cisco lightweight access point:

```
Switch# show ap name 3502b service-policy
```

```
NAME: Cisco AP      , DESCR: Cisco Wireless Access Point
PID: 3502I   , VID: V01, SN: FTX1525E94A
```

```
NAME: Dot11Radio0   , DESCR: 802.11N 2.4GHz Radio
PID: UNKNOWN, VID:   , SN: FOC1522BLNA
```

```
NAME: Dot11Radio1   , DESCR: 802.11N 5GHz Radio
PID: UNKNOWN, VID:   , SN: FOC1522BLNA
```

## show ap name dot11

To display 802.11a or 802.11b configuration information that corresponds to specific Cisco lightweight access points, use the **show ap name dot11** command.

```
show ap name ap-name dot11 {24ghz|5ghz} {ccx|cdp|profile|service-policy output|stats|tsm {all|client-mac}}
```

**Syntax Description**

<i>ap-name</i>	Name of the Cisco lightweight access point.
<b>24ghz</b>	Displays the 2.4 GHz band.
<b>5ghz</b>	Displays the 5 GHz band.
<b>ccx</b>	Displays the Cisco Client eXtensions (CCX) radio management status information.
<b>cdp</b>	Displays Cisco Discovery Protocol (CDP) information.
<b>profile</b>	Displays configuration and statistics of 802.11 profiling.
<b>service-policy output</b>	Displays downstream service policy information.
<b>stats</b>	Displays Cisco lightweight access point statistics.

<b>tsm</b>	Displays 802.11 traffic stream metrics statistics.
<b>all</b>	Displays the list of all access points to which the client has associations.
<i>client-mac</i>	MAC address of the client.

**Command Default**

None

**Command Modes**

Any command mode

**Command History**

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

This example shows how to display the service policy that is associated with the access point:

```
Switch# show ap name test-ap dot11 24ghz service-policy output

Policy Name   : test-ap1
Policy State  : Installed
```

This example shows how to display the CCX RRM 802.11 configuration for a specific access point:

```
Switch# show ap name AP01 dot11 24ghz ccx
```

This example show how to display CDP information for a specific access point:

```
Switch# show ap name AP01 dot11 24ghz cdp

AP Name          AP CDP State
-----
AP03              Disabled
```

This example show how to display the configuration and statistics of 802.11b profiling for a specific access point:

```
Switch# show ap name AP01 dot11 24ghz profile

802.11b Cisco AP performance profile mode           : GLOBAL
802.11b Cisco AP Interference threshold             : 10 %
802.11b Cisco AP noise threshold                    : -70 dBm
802.11b Cisco AP RF utilization threshold           : 80 %
802.11b Cisco AP throughput threshold               : 1000000 bps
802.11b Cisco AP clients threshold                  : 12 clients
```

This example show how to display downstream service policy information for a specific access point:

```
Switch# show ap name AP01 dot11 24ghz service-policy output

Policy Name   : def-11gn
Policy State  : Installed
```

This example show how to display statistics for a specific access point:

```
Switch# show ap name AP01 dot11 24ghz stats

Number of Users.....: 0
```

```

TxFragmentCount.....: 0
MulticastTxFrameCnt.....: 0
FailedCount.....: 0
RetryCount.....: 0
MultipleRetryCount.....: 0
FrameDuplicateCount.....: 0
RtsSuccessCount.....: 0
RtsFailureCount.....: 0
AckFailureCount.....: 0
RxIncompleteFragment.....: 0
MulticastRxFrameCnt.....: 0
FcsErrorCount.....: 0
TxFrameCount.....: 0
WepUndecryptableCount.....: 0
TxFramesDropped.....: 0

Call Admission Control (CAC) Stats
  Voice Bandwidth in use(% of config bw).....: 0
  Video Bandwidth in use(% of config bw).....: 0
  Total BW in use for Voice(%).....: 0
  Total BW in use for SIP Preferred call(%).....: 0

Load based Voice Call Stats
  Total channel MT free.....: 0
  Total voice MT free.....: 0
  Na Direct.....: 0
  Na Roam.....: 0

WMM TSPEC CAC Call Stats
  Total num of voice calls in progress.....: 0
  Num of roaming voice calls in progress.....: 0
  Total Num of voice calls since AP joined.....: 0
  Total Num of roaming calls since AP joined.....: 0
  Total Num of exp bw requests received.....: 0
  Total Num of exp bw requests admitted.....: 0
  Num of voice calls rejected since AP joined.....: 0
  Num of roam calls rejected since AP joined.....: 0
  Num of calls rejected due to insufficient bw.....: 0
  Num of calls rejected due to invalid params.....: 0
  Num of calls rejected due to PHY rate.....: 0
  Num of calls rejected due to QoS policy.....: 0

SIP CAC Call Stats
  Total Num of calls in progress.....: 0
  Num of roaming calls in progress.....: 0
  Total Num of calls since AP joined.....: 0
  Total Num of roaming calls since AP joined.....: 0
  Total Num of Preferred calls received.....: 0
  Total Num of Preferred calls accepted.....: 0
  Total Num of ongoing Preferred calls.....: 0
  Total Num of calls rejected(Insuff BW).....: 0
  Total Num of roam calls rejected(Insuff BW).....: 0

Band Select Stats
  Num of dual band client .....: 0
  Num of dual band client added.....: 0
  Num of dual band client expired .....: 0
  Num of dual band client replaced.....: 0
  Num of dual band client detected .....: 0
  Num of suppressed client .....: 0
  Num of suppressed client expired.....: 0
  Num of suppressed client replaced.....: 0

```

This example show how to display the traffic stream configuration for all clients that correspond to a specific access point:

```
Switch# show ap name AP01 dot11 24ghz tsm all
```

## show class-map

To display quality of service (QoS) class maps, which define the match criteria to classify traffic, use the **show class-map** command in EXEC mode.

**show class-map** [*class-map-name*]

### Syntax Description

<i>class-map-name</i>	(Optional) The class map name.
-----------------------	--------------------------------

### Command Modes

User EXEC  
Privileged EXEC

### Command History

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

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 Topics

[class-map](#), on page 16

## show wireless client calls

To display the total number of active or rejected calls on the switch, use the **show wireless client calls** command in privileged EXEC mode.

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

### Syntax Description

<b>active</b>	Displays active calls.
<b>rejected</b>	Displays rejected calls.

**Command Default** No default behavior or values.

**Command Modes** Privileged EXEC

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

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

```
switch# show wireless client calls active
TSPEC Calls:
-----
MAC Address      AP Name          Status           WLAN  Authenticated
-----
0000.1515.000f   AP-2             Associated        1    Yes
-----
SIP Calls:
-----
Number of Active TSPEC calls on 802.11a and 802.11b/g: 1
Number of Active SIP calls on 802.11a and 802.11b/g: 0
```

## show wireless client dot11

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

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

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

**Command Default** No default behavior or values.

**Command Modes** Privileged EXEC

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

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

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

  TSPEC Calls:
  -----

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

## show wireless client mac-address (Call Control)

To view call control information related to clients, use the **show wireless client mac-address** command in privileged EXEC mode.

**show wireless client mac-address** *mac-address* **call-control call-info**

Syntax Description		
	<i>mac-address</i>	The client MAC address.
	<b>call-control call-info</b>	Displays the call control and IP-related information about a client.

**Command Default** None

**Command Modes** Privileged EXEC

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

This example shows how to display call control and IP-related information about a client:

```
Switch# show wireless client mac-address 30e4.db41.6157 call-control call-info
Client MAC Address      : 30E4DB416157
```

```

Call 1 Statistics

Uplink IP Address      : 209.165.200.225
Downlink IP Address    : 209.165.200.226
Uplink Port            : 29052
Downlink Port          : 27538
Call ID                : c40acb4d-3b3b0.3d27da1e-356bed03
Called Party           : sip:1011
Calling Party          : sip:1012
Priority                : 6
Call On Hold           : false
Call Duration          : 30

Call 2 Statistics

No Active Call

```

## show wireless client mac-address (TCLAS)

To view information about TCLAS and user priority, use the **show wireless client mac-address** command in privileged EXEC mode.

**show wireless client mac-address** *mac-address* **tclas**

### Syntax Description

<i>mac-address</i>	The client MAC address.
<b>tclas</b>	Displays TCLAS and user priority-related information about a client.

### Command Modes

Privileged EXEC

### Command History

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

This example shows how to display the TCLAS and user priority-related information about a client:

```

Switch# show wireless client mac-address 30e4.db41.6157 tclas
MAC Address      UP TID Mask Source IP Addr  Dest IP Addr  SrcPort DstPort Proto
-----
30e4.db41.6157   4  4  95 167838052  2164326668   5060    5060    6
30e4.db41.6157   6  1  31 0          2164326668   0        27538   17

```

## show wireless client voice diagnostics

To display wireless client voice diagnostic parameters, use the **show wireless client voice diagnostics** command in privileged EXEC mode.

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

**Syntax Description**

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

**Command Default**

No default behavior or values.

**Command Modes**

Privileged EXEC

**Command History**

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

**Usage Guidelines**

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

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

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

## show policy-map

To display quality of service (QoS) policy maps, which define classification criteria for incoming traffic, use the **show policy-map** command in EXEC mode.

**show policy-map** [*policy-map-name*] **interface** *interface-id*

**Syntax Description**

<i>policy-map-name</i>	(Optional) Name of the policy-map.
<b>interface</b> <i>interface-id</i>	(Optional) Identifies the interface.



**Command Modes**

User EXEC  
Privileged EXEC

**Command History**

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.
Cisco IOS XE 3.3SE	The <b>interface</b> <i>interface-id</i> keyword was added.

**Usage Guidelines**

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

**Note**

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

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

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

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

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

GigabitEthernet1/0/1
Service-policy input: AutoQos-4.0-CiscoPhone-Input-Policy

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

```

exceeded 0 bytes; actions:
  set-dscp-transmit dscp table policed-dscp
  conformed 0000 bps, exceed 0000 bps

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

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

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

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

queue stats for all priority classes:
  Queueing
  priority level 1

  (total drops) 0
  (bytes output) 0

Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
  0 packets
  Match: dscp cs4 (32) cs5 (40) ef (46)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos 5
    0 packets, 0 bytes
    5 minute rate 0 bps
  Priority: 30% (300000 kbps), burst bytes 7500000,

  Priority Level: 1

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

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

  queue-buffers ratio 10

```

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

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

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

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

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

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

Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
  0 packets
  Match: dscp cs1 (8)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

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

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

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

Class-map: class-default (match-any)
  0 packets
  Match: any
```

```

    0 packets, 0 bytes
    5 minute rate 0 bps
Queueing

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

```

### Related Topics

[policy-map, on page 21](#)

## show wlan

To view WLAN parameters, use the **show wlan** command.

**show wlan** {**all** | **id** *wlan-id* | **name** *wlan-name* | **summary**}

### Syntax Description

<b>all</b>	Displays a summary of parameters of all configured WLANs. The list is ordered by the ascending order of the WLAN IDs.
<b>id</b> <i>wlan-id</i>	Specifies the wireless LAN identifier. The range is from 1 to 512.
<b>name</b> <i>wlan-name</i>	Specifies the WLAN profile name. The name is from 1 to 32 characters.
<b>summary</b>	Displays a summary of the parameters configured on a WLAN.

### Command Default

None

### Command Modes

Global configuration

### Command History

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

This example shows how to display a summary of the WLANs configured on the device:

```
Switch# show wlan summary
Number of WLANs: 1
```

```

WLAN Profile Name          SSID          VLAN Status
-----
45  test-wlan              test-wlan-ssid  1    UP

```

This example shows how to display a summary of parameters configured on a particular WLAN:

```
Switch# show wlan name test-wlan
WLAN Identifier                : 45
Profile Name                   : test-wlan
Network Name (SSID)           : test-wlan-ssid
Status                         : Enabled
Broadcast SSID                 : Enabled
Maximum number of Associated Clients : 0
AAA Policy Override            : Disabled
Network Admission Control
  NAC-State                    : Disabled
Number of Active Clients       : 0
Exclusionlist Timeout          : 60
Session Timeout                : 1800 seconds
CHD per WLAN                   : Enabled
Webauth DHCP exclusion        : Disabled
Interface                      : default
Interface Status               : Up
Multicast Interface            : test
WLAN IPv4 ACL                  : test
WLAN IPv6 ACL                  : unconfigured
DHCP Server                    : Default
DHCP Address Assignment Required : Disabled
DHCP Option 82                 : Disabled
DHCP Option 82 Format          : ap-mac
DHCP Option 82 Ascii Mode     : Disabled
DHCP Option 82 Rid Mode       : Disabled
QoS Service Policy - Input
  Policy Name                  : unknown
  Policy State                 : None
QoS Service Policy - Output
  Policy Name                  : unknown
  Policy State                 : None
QoS Client Service Policy
  Input Policy Name            : unknown
  Output Policy Name           : unknown
WifiDirect                     : Disabled
WMM                             : Disabled
Channel Scan Defer Priority:
  Priority (default)           : 4
  Priority (default)           : 5
  Priority (default)           : 6
Scan Defer Time (msecs)       : 100
Media Stream Multicast-direct  : Disabled
CCX - AironetIe Support       : Enabled
CCX - Gratuitous ProbeResponse (GPR) : Disabled
CCX - Diagnostics Channel Capability : Disabled
Dot11-Phone Mode (7920)      : Invalid
Wired Protocol                 : None
Peer-to-Peer Blocking Action   : Disabled
Radio Policy                   : All
DTIM period for 802.11a radio  : 1
DTIM period for 802.11b radio  : 1
Local EAP Authentication      : Disabled
Mac Filter Authorization list name : Disabled
Accounting list name           : Disabled
802.1x authentication list name : Disabled
Security
  802.11 Authentication        : Open System
  Static WEP Keys              : Disabled
  802.1X                       : Disabled
  Wi-Fi Protected Access (WPA/WPA2) : Enabled
    WPA (SSN IE)               : Disabled
    WPA2 (RSN IE)              : Enabled
      TKIP Cipher               : Disabled
      AES Cipher                : Enabled
    Auth Key Management
      802.1x                    : Enabled
      PSK                       : Disabled
      CCKM                     : Disabled
  IP Security                   : Disabled
  IP Security Passthru         : Disabled
```

```

L2TP : Disabled
Web Based Authentication : Disabled
Conditional Web Redirect : Disabled
Splash-Page Web Redirect : Disabled
Auto Anchor : Disabled
Sticky Anchoring : Enabled
Cranite Passthru : Disabled
Fortress Passthru : Disabled
PPTP : Disabled
Infrastructure MFP protection : Enabled
Client MFP : Optional
Webauth On-mac-filter Failure : Disabled
Webauth Authentication List Name : Disabled
Webauth Parameter Map : Disabled
Tkip MIC Countermeasure Hold-down Timer : 60
Call Snooping : Disabled
Passive Client : Disabled
Non Cisco WGB : Disabled
Band Select : Disabled
Load Balancing : Disabled
IP Source Guard : Disabled
Netflow Monitor : test
    Direction : Input
    Traffic : Datalink

Mobility Anchor List
IP Address
-----

```

## trust device

To configure trust for supported devices connected to an interface, use the **trust device** command in interface configuration mode. Use the **no** form of this command to disable trust for the connected device.

**trust device** {cisco-phone | cts | ip-camera | media-player}

**no trust device** {cisco-phone | cts | ip-camera | media-player}

### Syntax Description

<b>cisco-phone</b>	Configures a Cisco IP phone
<b>cts</b>	Configures a Cisco TelePresence System
<b>ip-camera</b>	Configures an IP Video Surveillance Camera (IPVSC)
<b>media-player</b>	Configures a Cisco Digital Media Player (DMP)

### Command Default

Trust disabled

### Command Modes

Interface configuration

### Command History

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

**Usage Guidelines**

Use the **trust device** command on the following types of interfaces:

- **Auto**— auto-template interface
- **Capwap**—CAPWAP tunnel interface
- **GigabitEthernet**—Gigabit Ethernet IEEE 802
- **GroupVI**—Group virtual interface
- **Internal Interface**—Internal interface
- **Loopback**—Loopback interface
- **Null**—Null interface
- **Port-channel**—Ethernet Channel interface
- **TenGigabitEthernet--10**—Gigabit Ethernet
- **Tunnel**—Tunnel interface
- **Vlan**—Catalyst VLANs
- **range—interface range** command

**Example**

The following example configures trust for a Cisco IP phone in Interface GigabitEthernet 1/0/1:

```
Switch(config)# interface GigabitEthernet1/0/1
Switch(config-if)# trust device cisco-phone
```

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







## Auto QoS Command Reference

- [auto qos classify](#), page 55
- [auto qos trust](#), page 60
- [auto qos video](#), page 67
- [auto qos voip](#) , page 77
- [show auto qos](#) , page 89

### 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

<b>police</b>	(Optional) Configure 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 XE 3.2SE	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	25 percent	15 percent
SRR shared	2	2, 3, 6,7	10 percent	25 percent	25 percent
SRR shared	3	0	60 percent	25 percent	40 percent
SRR shared	4	1	20 percent	25 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.

**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.

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.

The following policy maps and class maps are created and applied when running the **auto qos classify** and **auto qos classify police** commands:

Policy maps (For the **auto qos classify police** command):

- AutoQos-4.0-Classify-Police-Input-Policy
- AutoQos-4.0-Output-Policy

Class maps:

- AutoQos-4.0-Multimedia-Conf-Class (match-any)
- AutoQos-4.0-Bulk-Data-Class (match-any)
- AutoQos-4.0-Transaction-Class (match-any)
- AutoQos-4.0-Scavenger-Class (match-any)
- AutoQos-4.0-Signaling-Class (match-any)
- AutoQos-4.0-Default-Class (match-any)
- class-default (match-any)
- AutoQos-4.0-Output-Priority-Queue (match-any)
- AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
- AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
- AutoQos-4.0-Output-Trans-Data-Queue (match-any)
- AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
- AutoQos-4.0-Output-Scavenger-Queue (match-any)
- AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)

To disable auto-QoS on a port, use the **no auto qos classify** 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 classify** 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 example shows how to enable auto-QoS classification of an untrusted device and police traffic:

```
Switch(config)# interface gigabitEthernet1/0/6
Switch(config-if)# auto qos classify police
Switch(config-if)# end
Switch# show policy-map interface gigabitEthernet1/0/6

GigabitEthernet1/0/6

  Service-policy input: AutoQos-4.0-Classify-Police-Input-Policy

    Class-map: AutoQos-4.0-Multimedia-Conf-Class (match-any)
      0 packets
      Match: access-group name AutoQos-4.0-Acl-MultiEnhanced-Conf
        0 packets, 0 bytes
        5 minute rate 0 bps
      QoS Set
        dscp af41
      police:
        cir 5000000 bps, bc 156250 bytes
        conformed 0 bytes; actions:
          transmit
        exceeded 0 bytes; actions:
          drop
        conformed 0000 bps, exceed 0000 bps
```

```

Class-map: AutoQos-4.0-Bulk-Data-Class (match-any)
 0 packets
Match: access-group name AutoQos-4.0-Acl-Bulk-Data
 0 packets, 0 bytes
 5 minute rate 0 bps
QoS Set
 dscp af11
police:
  cir 10000000 bps, bc 312500 bytes
  conformed 0 bytes; actions:
   transmit
  exceeded 0 bytes; actions:
   set-dscp-transmit dscp table policed-dscp
  conformed 0000 bps, exceed 0000 bps

Class-map: AutoQos-4.0-Transaction-Class (match-any)
 0 packets
Match: access-group name AutoQos-4.0-Acl-Transactional-Data
 0 packets, 0 bytes
 5 minute rate 0 bps
QoS Set
 dscp af21
police:
  cir 10000000 bps, bc 312500 bytes
  conformed 0 bytes; actions:
   transmit
  exceeded 0 bytes; actions:
   set-dscp-transmit dscp table policed-dscp
  conformed 0000 bps, exceed 0000 bps

Class-map: AutoQos-4.0-Scavenger-Class (match-any)
 0 packets
Match: access-group name AutoQos-4.0-Acl-Scavenger
 0 packets, 0 bytes
 5 minute rate 0 bps
QoS Set
 dscp cs1
police:
  cir 10000000 bps, bc 312500 bytes
  conformed 0 bytes; actions:
   transmit
  exceeded 0 bytes; actions:
   drop
  conformed 0000 bps, exceed 0000 bps

Class-map: AutoQos-4.0-Signaling-Class (match-any)
 0 packets
Match: access-group name AutoQos-4.0-Acl-Signaling
 0 packets, 0 bytes
 5 minute rate 0 bps
QoS Set
 dscp cs3
police:
  cir 32000 bps, bc 8000 bytes
  conformed 0 bytes; actions:
   transmit
  exceeded 0 bytes; actions:
   drop
  conformed 0000 bps, exceed 0000 bps

Class-map: AutoQos-4.0-Default-Class (match-any)
 0 packets
Match: access-group name AutoQos-4.0-Acl-Default
 0 packets, 0 bytes
 5 minute rate 0 bps
QoS Set
 dscp default
police:
  cir 10000000 bps, bc 312500 bytes
  conformed 0 bytes; actions:
   transmit
  exceeded 0 bytes; actions:
   set-dscp-transmit dscp table policed-dscp

```

```

conformed 0000 bps, exceed 0000 bps

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

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

queue stats for all priority classes:
Queueing
priority level 1

(total drops) 0
(bytes output) 0

Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
 0 packets
Match: dscp cs4 (32) cs5 (40) ef (46)
 0 packets, 0 bytes
 5 minute rate 0 bps
Match: cos 5
 0 packets, 0 bytes
 5 minute rate 0 bps
Priority: 30% (300000 kbps), burst bytes 7500000,

Priority Level: 1

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

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

queue-buffers ratio 10

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

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

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

```

```

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

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

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

Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
 0 packets
Match: dscp cs1 (8)
 0 packets, 0 bytes
 5 minute rate 0 bps
Queueing

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

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

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

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

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

```

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

### Related Topics

[show auto qos , on page 89](#)

## 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**

<b>cos</b>	Trusts the CoS packet classification.
<b>dscp</b>	Trusts the DSCP packet classification.

**Command Default**

Auto-QoS trust is disabled on the port.

**Command Modes**

Interface configuration

**Command History**

Release	Modification
Cisco IOS XE 3.2SE	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 5: Traffic Types, Packet Labels, and Queues**

	VOIP Data Traffic	VOIP Control Traffic	Routing Protocol Traffic	STP <sup>1</sup> BPDU <sup>2</sup> Traffic	Real-Time Video Traffic	All Other Traffic	
DSCP <sup>3</sup>	46	24, 26	48	56	34	–	
CoS <sup>4</sup>	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)

<sup>1</sup> STP = Spanning Tree Protocol

<sup>2</sup> BPDU = bridge protocol data unit

<sup>3</sup> DSCP = Differentiated Services Code Point

<sup>4</sup> 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	25 percent	15 percent
SRR shared	2	2, 3, 6,7	10 percent	25 percent	25 percent
SRR shared	3	0	60 percent	25 percent	40 percent
SRR shared	4	1	20 percent	25 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.

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.

The following policy maps and class maps are created and applied when running the **auto qos trust cos** command:

Policy maps:

- AutoQos-4.0-Trust-Cos-Input-Policy
- AutoQos-4.0-Output-Policy

Class maps:

- class-default (match-any)
- AutoQos-4.0-Output-Priority-Queue (match-any)
- AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
- AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
- AutoQos-4.0-Output-Trans-Data-Queue (match-any)



- AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
- AutoQos-4.0-Output-Scavenger-Queue (match-any)
- AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)

The following policy maps and class maps are created and applied when running the **auto qos trust dscp** command:

Policy maps:

- AutoQos-4.0-Trust-Dscp-Input-Policy
- AutoQos-4.0-Output-Policy

Class maps:

- class-default (match-any)
- AutoQos-4.0-Output-Priority-Queue (match-any)
- AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
- AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
- AutoQos-4.0-Output-Trans-Data-Queue (match-any)
- AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
- AutoQos-4.0-Output-Scavenger-Queue (match-any)
- AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)

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).

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

```
Switch(config)# interface gigabitEthernet1/0/17
Switch(config-if)# auto qos trust cos
Switch(config-if)# end
Switch# show policy-map interface GigabitEthernet1/0/17

GigabitEthernet1/0/17

  Service-policy input: AutoQos-4.0-Trust-Cos-Input-Policy

    Class-map: class-default (match-any)
      0 packets
      Match: any
        0 packets, 0 bytes
        5 minute rate 0 bps
      QoS Set
        cos cos table AutoQos-4.0-Trust-Cos-Table

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

  queue stats for all priority classes:
    Queueing
    priority level 1

    (total drops) 0
```

```

(bytes output) 0

Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
 0 packets
 Match: dscp cs4 (32) cs5 (40) ef (46)
   0 packets, 0 bytes
   5 minute rate 0 bps
 Match: cos 5
   0 packets, 0 bytes
   5 minute rate 0 bps
 Priority: 30% (300000 kbps), burst bytes 7500000,

 Priority Level: 1

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

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

 queue-buffers ratio 10

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

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

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

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

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

```

```

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

Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
 0 packets
Match: dscp cs1 (8)
 0 packets, 0 bytes
 5 minute rate 0 bps
Queueing

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

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

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

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

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

```

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

```

Switch(config)# interface GigabitEthernet1/0/18
Switch(config-if)# auto qos trust dscp
Switch(config-if)# end
Switch#show policy-map interface GigabitEthernet1/0/18

GigabitEthernet1/0/18

Service-policy input: AutoQos-4.0-Trust-Dscp-Input-Policy

Class-map: class-default (match-any)
 0 packets
Match: any
 0 packets, 0 bytes
 5 minute rate 0 bps
QoS Set
 dscp dscp table AutoQos-4.0-Trust-Dscp-Table

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

queue stats for all priority classes:
Queueing
priority level 1

(total drops) 0
(bytes output) 0

Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)

```

```

0 packets
Match: dscp cs4 (32) cs5 (40) ef (46)
  0 packets, 0 bytes
  5 minute rate 0 bps
Match: cos 5
  0 packets, 0 bytes
  5 minute rate 0 bps
Priority: 30% (300000 kbps), burst bytes 7500000,

Priority Level: 1

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

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

queue-buffers ratio 10

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

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

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

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

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

(total drops) 0
(bytes output) 0

```

```

bandwidth remaining 4%
queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
 0 packets
Match: dscp cs1 (8)
 0 packets, 0 bytes
 5 minute rate 0 bps
Queueing

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

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

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

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

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

```

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

### Related Topics

[show auto qos , on page 89](#)

## 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

<b>cts</b>	Specifies a port connected to a Cisco TelePresence System and automatically configures QoS for video.
<b>ip-camera</b>	Specifies a port connected to a Cisco IP camera and automatically configures QoS for video.

---

<b>media-player</b>	Specifies a port 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.

**Command Modes** Interface configuration

**Command History**

---

<b>Release</b>	<b>Modification</b>
Cisco IOS XE 3.2SE	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. 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 the queue tables at the end of this section.

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

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.

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.

The following policy maps and class maps are created and applied when running the **auto qos video cts** command:

Policy maps:

- AutoQos-4.0-Trust-Cos-Input-Policy

- AutoQos-4.0-Output-Policy

#### Class maps

- class-default (match-any)
- AutoQos-4.0-Output-Priority-Queue (match-any)
- AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
- AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
- AutoQos-4.0-Output-Trans-Data-Queue (match-any)
- AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
- AutoQos-4.0-Output-Scavenger-Queue (match-any)
- AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)

The following policy maps and class maps are created and applied when running the **auto qos video ip-camera** command:

#### Policy maps:

- AutoQos-4.0-Trust-Dscp-Input-Policy
- AutoQos-4.0-Output-Policy

#### Class maps:

- class-default (match-any)
- AutoQos-4.0-Output-Priority-Queue (match-any)
- AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
- AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
- AutoQos-4.0-Output-Trans-Data-Queue (match-any)
- AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
- AutoQos-4.0-Output-Scavenger-Queue (match-any)
- AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)

The following policy maps and class maps are created and applied when running the **auto qos video media-player** command:

#### Policy maps:

- AutoQos-4.0-Trust-Dscp-Input-Policy
- AutoQos-4.0-Output-Policy

#### Class maps:

- class-default (match-any)
- AutoQos-4.0-Output-Priority-Queue (match-any)
- AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)

- AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
- AutoQos-4.0-Output-Trans-Data-Queue (match-any)
- AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
- AutoQos-4.0-Output-Scavenger-Queue (match-any)
- AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)

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).

**Table 7: Traffic Types, Packet Labels, and Queues**

	VOIP Data Traffic	VOIP Control Traffic	Routing Protocol Traffic	STP <sup>5</sup> BPDUs <sup>6</sup>	Real-Time Video Traffic	All Other Traffic	
DSCP <sup>7</sup>	46	24, 26	48	56	34	–	
CoS <sup>8</sup>	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)

<sup>5</sup> STP = Spanning Tree Protocol

<sup>6</sup> BPDUs = bridge protocol data unit

<sup>7</sup> DSCP = Differentiated Services Code Point

<sup>8</sup> 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	25 percent	15 percent
SRR shared	2	2, 3, 6, 7	10 percent	25 percent	25 percent
SRR shared	3	0	60 percent	25 percent	40 percent
SRR shared	4	1	20 percent	25 percent	20 percent



The following is an example of the **auto qos video cts** command and the applied policies and class maps:

```
Switch(config)# interface gigabitEthernet1/0/12
Switch(config-if)# auto qos video cts
Switch(config-if)# end
Switch# show policy-map interface gigabitEthernet1/0/12

GigabitEthernet1/0/12

  Service-policy input: AutoQos-4.0-Trust-Cos-Input-Policy

    Class-map: class-default (match-any)
      0 packets
      Match: any
        0 packets, 0 bytes
        5 minute rate 0 bps
      QoS Set
        cos cos table AutoQos-4.0-Trust-Cos-Table

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

    queue stats for all priority classes:
      Queueing
      priority level 1

      (total drops) 0
      (bytes output) 0

    Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
      0 packets
      Match: dscp cs4 (32) cs5 (40) ef (46)
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: cos 5
        0 packets, 0 bytes
        5 minute rate 0 bps
      Priority: 30% (300000 kbps), burst bytes 7500000,

      Priority Level: 1

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

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

      queue-buffers ratio 10

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

      (total drops) 0
      (bytes output) 0
```

```

bandwidth remaining 10%
queue-buffers ratio 10

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

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

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

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

Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
 0 packets
Match: dscp cs1 (8)
 0 packets, 0 bytes
 5 minute rate 0 bps
Queueing

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

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

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

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

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

```

The following is an example of the **auto qos video ip-camera** command and the applied policies and class maps:

```
Switch(config)# interface GigabitEthernet1/0/9
Switch(config-if)# auto qos video ip-camera
Switch(config-if)# end
Switch# show policy-map interface GigabitEthernet1/0/9

GigabitEthernet1/0/9

  Service-policy input: AutoQos-4.0-Trust-Dscp-Input-Policy

    Class-map: class-default (match-any)
      0 packets
      Match: any
        0 packets, 0 bytes
        5 minute rate 0 bps
      QoS Set
        dscp dscp table AutoQos-4.0-Trust-Dscp-Table

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

    queue stats for all priority classes:
      Queueing
      priority level 1

      (total drops) 0
      (bytes output) 0

    Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
      0 packets
      Match: dscp cs4 (32) cs5 (40) ef (46)
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: cos 5
        0 packets, 0 bytes
        5 minute rate 0 bps
      Priority: 30% (300000 kbps), burst bytes 7500000,

      Priority Level: 1

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

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

      queue-buffers ratio 10

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

```

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

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

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

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

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

Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
 0 packets
Match: dscp cs1 (8)
 0 packets, 0 bytes
 5 minute rate 0 bps
Queueing

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

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

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

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

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

```

The following is an example of the **auto qos video media-player** command and the applied policies and class maps.

```
Switch(config)# interface GigabitEthernet1/0/7
Switch(config-if)# auto qos video media-player
Switch(config-if)# end
Switch# show policy-map interface GigabitEthernet1/0/7

GigabitEthernet1/0/7

  Service-policy input: AutoQos-4.0-Trust-Dscp-Input-Policy

    Class-map: class-default (match-any)
      0 packets
      Match: any
        0 packets, 0 bytes
        5 minute rate 0 bps
      QoS Set
        dscp dscp table AutoQos-4.0-Trust-Dscp-Table

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

    queue stats for all priority classes:
      Queueing
      priority level 1

      (total drops) 0
      (bytes output) 0

    Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
      0 packets
      Match: dscp cs4 (32) cs5 (40) ef (46)
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: cos 5
        0 packets, 0 bytes
        5 minute rate 0 bps
      Priority: 30% (300000 kbps), burst bytes 7500000,

      Priority Level: 1

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

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

      queue-buffers ratio 10

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

```

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

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

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

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

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

Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
 0 packets
Match: dscp cs1 (8)
 0 packets, 0 bytes
 5 minute rate 0 bps
Queueing

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

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

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

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

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

```

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

### Related Topics

[show auto qos](#) , on page 89

## 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

<b>cisco-phone</b>	Specifies a port 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.
<b>cisco-softphone</b>	Specifies a port connected to a device running the Cisco SoftPhone, and automatically configures QoS for VoIP.
<b>trust</b>	Specifies a port 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, to assign packet labels, and to configure the ingress and egress queues.

### Command Default

Interface configuration

### Command History

Release	Modification
Cisco IOS XE 3.2SE	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 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, you should enable auto-QoS before you configure other QoS commands. You can fine-tune the auto-QoS configuration *after* you enable auto-QoS.

**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 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 those traffic matching 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.

The following policy maps and class maps are created and applied when running the **auto qos voip trust** command:

Policy maps:

- AutoQos-4.0-Trust-Cos-Input-Policy
- AutoQos-4.0-Output-Policy

Class maps:

- class-default (match-any)
- AutoQos-4.0-Output-Priority-Queue (match-any)
- AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
- AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
- AutoQos-4.0-Output-Trans-Data-Queue (match-any)
- AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
- AutoQos-4.0-Output-Scavenger-Queue (match-any)
- AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)

The following policy maps and class maps are created and applied when running the **auto qos voip cisco-softphone** command:

Policy maps:

- AutoQos-4.0-CiscoSoftPhone-Input-Policy
- AutoQos-4.0-Output-Policy

Class maps:

- AutoQos-4.0-Voip-Data-Class (match-any)
- AutoQos-4.0-Voip-Signal-Class (match-any)
- AutoQos-4.0-Multimedia-Conf-Class (match-any)
- AutoQos-4.0-Bulk-Data-Class (match-any)
- AutoQos-4.0-Transaction-Class (match-any)
- AutoQos-4.0-Scavenger-Class (match-any)
- AutoQos-4.0-Signaling-Class (match-any)
- AutoQos-4.0-Default-Class (match-any)
- class-default (match-any)
- AutoQos-4.0-Output-Priority-Queue (match-any)
- AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)

- AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
- AutoQos-4.0-Output-Trans-Data-Queue (match-any)
- AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
- AutoQos-4.0-Output-Scavenger-Queue (match-any)
- AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)

The following policy maps and class maps are created and applied when running the **auto qos voip cisco-phone** command:

Policy maps:

- service-policy input AutoQos-4.0-CiscoPhone-Input-Policy
- service-policy output AutoQos-4.0-Output-Policy

Class maps:

- class AutoQos-4.0-Voip-Data-CiscoPhone-Class
- class AutoQos-4.0-Voip-Signal-CiscoPhone-Class
- class AutoQos-4.0-Default-Class

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).

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

**Table 9: 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	25 percent	15 percent
SRR shared	2	2, 3, 6, 7	10 percent	25 percent	25 percent
SRR shared	3	0	60 percent	25 percent	40 percent
SRR shared	4	1	20 percent	25 percent	20 percent

The following is an example of the **auto qos voip trust** command and the applied policies and class maps:

```
Switch(config)# interface gigabitEthernet1/0/31
Switch(config-if)# auto qos voip trust
Switch(config-if)# end
```

```

Switch# show policy-map interface GigabitEthernet1/0/31
GigabitEthernet1/0/31
  Service-policy input: AutoQos-4.0-Trust-Cos-Input-Policy
    Class-map: class-default (match-any)
      0 packets
      Match: any
        0 packets, 0 bytes
        5 minute rate 0 bps
      QoS Set
        cos cos table AutoQos-4.0-Trust-Cos-Table
  Service-policy output: AutoQos-4.0-Output-Policy
    queue stats for all priority classes:
      Queueing
        priority level 1

      (total drops) 0
      (bytes output) 0

    Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
      0 packets
      Match: dscp cs4 (32) cs5 (40) ef (46)
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: cos 5
        0 packets, 0 bytes
        5 minute rate 0 bps
      Priority: 30% (300000 kbps), burst bytes 7500000,

      Priority Level: 1

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

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

      queue-buffers ratio 10

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

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

    Class-map: AutoQos-4.0-Output-Trans-Data-Queue (match-any)
      0 packets
      Match: dscp af21 (18) af22 (20) af23 (22)

```

```

    0 packets, 0 bytes
    5 minute rate 0 bps
Match: cos 2
    0 packets, 0 bytes
    5 minute rate 0 bps
Queueing

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

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

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

Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
0 packets
Match: dscp cs1 (8)
    0 packets, 0 bytes
    5 minute rate 0 bps
Queueing

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

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

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

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

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

```

The following is an example of the **auto qos voip cisco-phone** command and the applied policies and class maps:

```

Switch(config)# interface gigabitEthernet1/0/5
Switch(config-if)# auto qos voip cisco-phone
Switch(config-if)# end
Switch# show policy-map interface gigabitEthernet1/0/5

```

GigabitEthernet1/0/5

```

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

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

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

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

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

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

queue stats for all priority classes:
  Queueing
  priority level 1

  (total drops) 0
  (bytes output) 0

Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
  0 packets
  Match: dscp cs4 (32) cs5 (40) ef (46)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos 5
    0 packets, 0 bytes
    5 minute rate 0 bps
  Priority: 30% (300000 kbps), burst bytes 7500000,

  Priority Level: 1

Class-map: AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
  0 packets
  Match: dscp cs2 (16) cs3 (24) cs6 (48) cs7 (56)
    0 packets, 0 bytes

```

```

    5 minute rate 0 bps
  Match: cos 3
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing
  queue-limit dscp 16 percent 80
  queue-limit dscp 24 percent 90
  queue-limit dscp 48 percent 100
  queue-limit dscp 56 percent 100

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

  queue-buffers ratio 10

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

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

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

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

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

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

Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
  0 packets
  Match: dscp cs1 (8)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

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

```

```

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

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

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

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

```

The following is an example of the **auto qos voip cisco-softphone** command and the applied policies and class maps:

```

Switch(config)# interface gigabitEthernet1/0/20
Switch(config-if)# auto qos voip cisco-softphone
Switch(config-if)# end
Switch# show policy-map interface gigabitEthernet1/0/20

GigabitEthernet1/0/20

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

Class-map: AutoQos-4.0-Voip-Data-Class (match-any)
  0 packets
  Match: dscp ef (46)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos 5
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
  dscp ef
  police:
    cir 128000 bps, bc 8000 bytes
    conformed 0 bytes; actions:
      transmit
    exceeded 0 bytes; actions:
      set-dscp-transmit dscp table policed-dscp
    conformed 0000 bps, exceed 0000 bps

Class-map: AutoQos-4.0-Voip-Signal-Class (match-any)
  0 packets
  Match: dscp cs3 (24)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos 3
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
  dscp cs3
  police:
    cir 32000 bps, bc 8000 bytes
    conformed 0 bytes; actions:
      transmit
    exceeded 0 bytes; actions:
      set-dscp-transmit dscp table policed-dscp
    conformed 0000 bps, exceed 0000 bps

```

```

Class-map: AutoQos-4.0-Multimedia-Conf-Class (match-any)
  0 packets
  Match: access-group name AutoQos-4.0-Acl-MultiEnhanced-Conf
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
    dscp af41
  police:
    cir 5000000 bps, bc 156250 bytes
    conformed 0 bytes; actions:
      transmit
    exceeded 0 bytes; actions:
      drop
    conformed 0000 bps, exceed 0000 bps

Class-map: AutoQos-4.0-Bulk-Data-Class (match-any)
  0 packets
  Match: access-group name AutoQos-4.0-Acl-Bulk-Data
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
    dscp af11
  police:
    cir 10000000 bps, bc 312500 bytes
    conformed 0 bytes; actions:
      transmit
    exceeded 0 bytes; actions:
      set-dscp-transmit dscp table policed-dscp
    conformed 0000 bps, exceed 0000 bps

Class-map: AutoQos-4.0-Transaction-Class (match-any)
  0 packets
  Match: access-group name AutoQos-4.0-Acl-Transactional-Data
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
    dscp af21
  police:
    cir 10000000 bps, bc 312500 bytes
    conformed 0 bytes; actions:
      transmit
    exceeded 0 bytes; actions:
      set-dscp-transmit dscp table policed-dscp
    conformed 0000 bps, exceed 0000 bps

Class-map: AutoQos-4.0-Scavenger-Class (match-any)
  0 packets
  Match: access-group name AutoQos-4.0-Acl-Scavenger
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
    dscp cs1
  police:
    cir 10000000 bps, bc 312500 bytes
    conformed 0 bytes; actions:
      transmit
    exceeded 0 bytes; actions:
      drop
    conformed 0000 bps, exceed 0000 bps

Class-map: AutoQos-4.0-Signaling-Class (match-any)
  0 packets
  Match: access-group name AutoQos-4.0-Acl-Signaling
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
    dscp cs3
  police:
    cir 32000 bps, bc 8000 bytes
    conformed 0 bytes; actions:
      transmit
    exceeded 0 bytes; actions:

```



```

        drop
        conformed 0000 bps, exceed 0000 bps

Class-map: AutoQos-4.0-Default-Class (match-any)
  0 packets
  Match: access-group name AutoQos-4.0-Acl-Default
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
    dscp default
  police:
    cir 10000000 bps, bc 312500 bytes
    conformed 0 bytes; actions:
      transmit
    exceeded 0 bytes; actions:
      set-dscp-transmit dscp table policed-dscp
    conformed 0000 bps, exceed 0000 bps

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

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

queue stats for all priority classes:
  Queueing
    priority level 1

    (total drops) 0
    (bytes output) 0

Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
  0 packets
  Match: dscp cs4 (32) cs5 (40) ef (46)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos 5
    0 packets, 0 bytes
    5 minute rate 0 bps
  Priority: 30% (300000 kbps), burst bytes 7500000,

  Priority Level: 1

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

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

    queue-buffers ratio 10

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

```

```

Queueing

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

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

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

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

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

Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
0 packets
Match: dscp cs1 (8)
  0 packets, 0 bytes
  5 minute rate 0 bps
Queueing

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

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

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

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

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

```

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

### Related Topics

[show auto qos](#) , on page 89

## show auto qos

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

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

### Syntax Description

<b>interface</b> [ <i>interface-id</i> ]	(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 XE 3.2SE	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.

Beginning in Cisco IOS Release 12.2(40)SE, the **show auto qos** command output shows the service policy information for the Cisco IP phone.

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 auto qos interface** *interface-id* command when the **auto qos voip cisco-phone** interface configuration command is entered:

```
Switch# show auto qos interface gigabitethernet1/0/2
GigabitEthernet1/0/2
auto qos voip cisco-phone
```

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
```



## INDEX

### A

auto qos classify command [55](#)  
auto qos trust command [60](#)  
auto qos video command [67](#)  
auto qos voip command [77](#)

### C

class command [14](#)  
class-map command [16](#)

### M

match (class-map configuration) command [17](#)  
match non-client-nrt command [20](#)  
match wlan user-priority command [21](#)

### P

policy-map command [21](#)

### Q

queue-limit command [27](#)

### S

service-policy command [29, 31](#)  
set command [32](#)  
show ap name dot11 [39](#)  
show ap name service-policy [38](#)  
show auto qos command [89](#)  
show class-map command [42](#)  
show policy-map command [46](#)  
show wireless client calls command [42](#)  
show wireless client dot11 command [43](#)  
show wireless client mac-address command [44, 45](#)  
show wireless client voice diagnostics command [45](#)  
show wlan command [50](#)

