



# CHAPTER 53

## Using Automatic QoS

---

This chapter describes how to use the automatic quality of service (QoS) configuration features on the Catalyst 6500 series switches.

**Note**

For complete syntax and usage information for the commands that are used in this chapter, refer to the *Catalyst 6500 Series Switch Command Reference* publication.

---

**Note**

Automatic QoS is not supported on Supervisor Engine 720 in software release 8.1(1).

---

**Note**

For information on using automatic voice configuration, see the “[Using SmartPorts](#)” section on [page 55-38](#).

---

This chapter consists of these sections:

- [Understanding How Automatic QoS Works, page 53-1](#)
- [QoS Overview, page 53-2](#)
- [Using the Automatic QoS Macro on the Switch, page 53-3](#)
- [Using Automatic QoS in Your Network, page 53-28](#)

## Understanding How Automatic QoS Works

Automatic QoS consists of a macro that simplifies the QoS configuration on the Catalyst 6500 series switches. The automatic QoS macro covers all the QoS configuration tasks that are required for implementing the recommended Architecture for Voice, Video, and Integrated Data (AVVID) settings for a voice port.

Automatic QoS focuses on the voice networks that are built using the Cisco IP Phone 79xx series and the Cisco SoftPhone. However, other phones can equally benefit from the automatically configured QoS settings. With automatic QoS, you use keywords, such as **ciscoipphone** or **ciscosoftphone**, or other AVVID types to allow you to specify the type of QoS parameters that you desire on a particular port. With automatic QoS, all appropriate QoS settings (Internet Engineering Task Force (IETF)-recommended values and proven AVVID settings) are applied to the port.

# QoS Overview

These sections provide an overview of QoS:

- [Typical CoS and DSCP Values for Voice and Video Networks, page 53-2](#)
- [QoS Scenario—Cisco IP Phone, page 53-3](#)
- [QoS Scenario—Cisco SoftPhone, page 53-3](#)

## Typical CoS and DSCP Values for Voice and Video Networks

The IETF recommends that you use several values for the different traffic types that are found in voice and video networks. Automatic QoS uses these values to configure such QoS parameters as CoS-to-queue maps, differentiated services code point (DSCP)-to-CoS maps, and so on.

Catalyst 6500 series switches use the differentiated services (DIFFSERV) model for QoS. This model outlines three traffic types:

- EF (Expedited Forwarding)
- AF (Assured Forwarding)
- BE (Best Effort)

Four traffic classes exist within the AF class. The classes are denoted by AFX $Y$  where  $X$  is the class number and  $Y$  is the drop precedence number.  $X$  corresponds to a queue, and  $Y$  corresponds to a drop precedence value within the queue (either WRED or tail drop). EF has the highest priority, BE has the lowest priority, and the priority for AF is somewhere in between.

See [Table 53-1](#) for the recommended CoS and DSCP values for the voice networks and other traffic types. The values listed are assumed when configuring the CoS-to-queue maps and other CoS/DSCP value-dependent configurations with the automatic QoS macro.

**Table 53-1** Typical CoS and DSCP values in Cisco Voice and Video Networks

CoS Value <sup>1</sup>	DSCP	Significance
0	0	Default traffic (BE class)
3	26 (IETF recommended)	Voice/video call control/signaling (TCP) AF31 class
5	46 (IETF recommended)	Voice-bearer stream (RTP/UDP) EF class
4	34 (IETF recommended)	Video-bearer stream AF41 class
2	18	Mission critical/transactional traffic AF21 class
1	10	Streaming video (not interactive) AF11
6	48	Routing protocols (as default)
7		Spanning Tree Protocol

1. Some values differ from the current QoS default values for Catalyst software (such as CoS-to-DSCP maps).

The priorities for these CoS/DSCP values are as follows:

- CoS 5 (voice data)—Highest priority (priority queue if present, otherwise high queue)
- CoS 6, 7 (routing protocols)—Second priority (high queue)
- CoS 3, 4 (call signal and video stream)—Third priority (high queue)
- CoS 1, 2 (streaming and mission critical)—Fourth priority (high queue)
- CoS 0— Low priority (low queue)

For the ports that do not implement a priority queue, the WRED and tail-drop mechanisms are used to attain traffic prioritization within the queue. See the [“Global Automatic QoS Detail Settings”](#) section on [page 53-7](#) for specific scheduling settings.

## QoS Scenario—Cisco IP Phone

In most configurations, you can connect the Cisco IP Phone 79xx directly to the Catalyst switch port. Optionally, you can attach a PC to the phone and use the phone as a hop to the switch.

Typically, the traffic that comes from the phone and enters the switch is marked with a tag using the 802.1Q/p header. The header contains the VLAN information and the CoS 3-bit field. The CoS determines the priority of the packet. The switch uses the CoS field to distinguish the PC traffic from the phone traffic. The switch can also use the DSCP field for the same purpose.

In most Cisco IP Phone 79xx configurations, the traffic that comes from the phone and enters the switch is trusted. You set the port trust to trust-cos to prioritize the voice traffic over other types of traffic in the network.

The Cisco IP Phone 79xx has a built-in switch that mixes the traffic that comes from the PC, the phone, and the switch port. The Cisco IP Phone 79xx has the trust and classification capabilities that you need to configure. For more information, see the [“Port-Specific Automatic QoS Settings—ciscosoftphone”](#) section on [page 53-10](#).

## QoS Scenario—Cisco SoftPhone

The Cisco SoftPhone is a software product that runs on a standard PC and emulates an IP phone. The main difference between the Cisco SoftPhone and the Cisco IP Phone 79xx is that the Cisco SoftPhone marks its voice traffic through a DSCP, while the Cisco IP Phone 79xx marks its traffic through a CoS. The QoS settings on the switch accommodate this behavior by trusting the Layer 3 marking of the traffic entering the port. All other behavior is similar to the Cisco IP Phone 79xx.

# Using the Automatic QoS Macro on the Switch

These sections describe the automatic QoS macro:

- [Automatic QoS Overview, page 53-4](#)
- [Automatic QoS Configuration Guidelines and Restrictions, page 53-4](#)
- [Global Automatic QoS Macro, page 53-6](#)
- [Port-Specific Automatic QoS Macro, page 53-9](#)
- [CLI Interface for Automatic QoS, page 53-13](#)
- [Detailed Automatic QoS Configuration Statements, page 53-18](#)

- [Warning and Error Conditions, page 53-23](#)
- [syslog Additions, page 53-25](#)
- [Other Relevant syslog Messages, page 53-26](#)
- [Summary of Automatic QoS Features, page 53-27](#)

## Automatic QoS Overview

The automatic QoS macro is divided into these two separate components:

- Global automatic QoS command (**set qos auto**)—Deals with all switch-wide related QoS settings that are not specific to any given interface. These settings include CoS-to-queue maps, CoS-to-DSCP maps, and WRED settings for specific port types and global mappings.
- Port-specific automatic QoS command (**set port qos mod/port autoqos**)—Configures all inbound QoS parameters for a particular port to reflect the desired traffic type (voice, video, and applications).



**Tip**

---

To ensure that automatic QoS works properly, you should execute both components.

---

## Automatic QoS Configuration Guidelines and Restrictions

These sections provide the configuration guidelines and restrictions for automatic QoS:

- [Configuration Files, page 53-4](#)
- [Supported Phones, page 53-5](#)
- [CDP Dependencies, page 53-5](#)
- [COPS Considerations, page 53-5](#)
- [RSVP Considerations, page 53-5](#)
- [Current QoS Default Settings, page 53-6](#)
- [EtherChannel Considerations, page 53-6](#)
- [Video Traffic Considerations, page 53-6](#)
- [Clearing the QoS Configuration, page 53-6](#)
- [PFC/PFC2 Support, page 53-6](#)
- [1p1q0t/1p3q1t Port Support, page 53-6](#)

## Configuration Files

Creating the commands (macros) that implement other commands can lead to conflicting commands. For example, if you configure a CoS-to-queue map with a certain setting and then enable the automatic QoS macro feature, the macro that you enabled will alter the CoS-to-queue map.

To avoid conflicting commands, the configuration file includes all the legacy commands that are included in the macro. The actual macro command does not appear in the configuration file; instead, all the existing configuration commands that result from executing the macro are included in the configuration file. For example, when you enter the **set qos autoqos** command and then enter the **write config** command, all existing QoS-related CLI commands display, excluding the actual macro command itself.

## Supported Phones

When you use automatic QoS with the **ciscoipphone** keyword, some of the QoS configuration requires phone-specific configuration (trust-ext, ext-cos) which is supported only on the following phones: Cisco IP Phone 7910, Cisco IP Phone 7940, Cisco IP Phone 7960, and Cisco IP Phone 7935. However, the **ciscoipphone** keyword is not exclusive to these models only; any phone can benefit from all the other QoS settings that are configured on the switch.

Cisco SoftPhone is supported through the **ciscoipsoftphone** keyword.

## CDP Dependencies

To configure the QoS settings and trusted boundary on the Cisco IP Phone, you must enable Cisco Discovery Protocol (CDP) version 2 or later on the port. If you enable trusted boundary, a syslog warning message displays if CDP is not enabled or if CDP is running version 1.

You need to enable CDP only for the **ciscoipphone** QoS configuration; CDP does not affect the other components of the automatic QoS features. When you use the **ciscoipphone** keyword with the port-specific automatic QoS feature, a warning displays if the port does not have CDP enabled. See the [“CDP Warning” section on page 53-24](#).

## COPS Considerations

You can configure a port for the local policy or the Common Open Policy Service (COPS) policy. This setting specifies whether the port should get its QoS configuration information from a local configuration or through a COPS server. If you enable COPS on the port as well as globally enable COPS, the policy that is specified by the COPS server applies. If you disable COPS and/or the configured policy is local, the local configuration QoS policy applies.

Automatic QoS affects only the local policy on a port. If you execute automatic QoS on a port that has a configured policy that is currently set to COPS, the policy reverts to the local policy. The global QoS policy reverts to the local policy (through the global automatic QoS command), and the port-based policy reverts to the local policy (through the port-based automatic QoS command). A warning displays if the policy of a port or global policy has been changed from COPS to local. For more information, see the [“COPS Warning Message” section on page 53-24](#). Any existing COPS roles that are already associated with the port are not changed.

## RSVP Considerations

All global and port-based Resource Reservation Protocol (RSVP)-related settings (including the RSVP [Designated Subnet Bandwidth Manager] DBSM election settings) are not changed by the automatic QoS macros.

## Current QoS Default Settings

All current QoS settings are applied as described in the “[Detailed Automatic QoS Configuration Statements](#)” section on page 53-18. Some of these QoS settings reflect the current QoS defaults. After automatic QoS has been applied, *all* QoS settings, regardless of whether or not they were defaults, are applied on the port/switch.

## EtherChannel Considerations

The global automatic QoS command supports channeling. All outbound QoS is configured for all channeling or nonchanneling interfaces. Channeling is not supported with the per-port automatic QoS commands.

## Video Traffic Considerations

The CoS and DSCP values that are associated with the video traffic are prioritized for the global QoS settings. For more information, see the “[Typical CoS and DSCP Values for Voice and Video Networks](#)” section on page 53-2.

## Clearing the QoS Configuration

Clearing the QoS configuration resets the configuration to the default QoS values. The automatic QoS features do not alter the default values.

## PFC/PFC2 Support

No PFC or PFC2 is required for the **ciscoipphone** and **trust cos** keywords. A PFC or PFC2 is required for the **ciscosoftphone** and **trust dscp** keywords.

## 1p1q0t/1p3q1t Port Support

All 1p1q0t/1p3q1t ports must either be in port-based mode or VLAN-based mode. If a change is required (for example, if the port was configured for VLAN-based mode before you executed automatic QoS), a syslog message displays. The message indicates that a change to an interface type was needed that affected all ports in the module. For more information, see the “[Interface Change for All Ports Required—Warning Level](#)” section on page 53-26.

## Global Automatic QoS Macro

These sections describe the global automatic QoS macro:

- [Overview, page 53-7](#)
- [Global Automatic QoS Detail Settings, page 53-7](#)

## Overview

You must configure both egress and ingress QoS for QoS to function properly. Because any traffic type can egress on any given port, the egress QoS settings must have global QoS settings. The settings take into account *all* the possible traffic types that are listed in the “[Typical CoS and DSCP Values for Voice and Video Networks](#)” section on page 53-2. The egress QoS settings are applied to all the ports in the switch. The global QoS settings cover the *ingress* scheduling settings, because the granularity CoS-to-queue mapping is *port-type* specific and not port specific. The port-specific QoS settings, such as QoS ACLs, port trust, and default CoS, are not altered.

## Global Automatic QoS Detail Settings

Table 53-2 through Table 53-6 list the values of all the QoS parameters that are configured through the global automatic QoS command.



### Note

The 1p1q8t default WRED settings are not changed from the current QoS defaults; only the CoS-to-threshold map is changed.

**Table 53-2 Switch-Wide Settings (Global QoS Settings)**

QoS Parameter	Setting
CoS-to-DSCP map	0 <b>10 18 26 34 46</b> 48 56 (bold indicates nondefault values)
IP-precedence-to-DSCP map	0 <b>10 18 26 34 46</b> 48 56 (bold indicates nondefault values)
DSCP-to-CoS map	{0-7}, {8-15}, {16-23}, {24-31}, {32-39}, {40-47}, {48-55}, {56-63} (as per default)
Policed-DSCP map	As per default with 46:0 and 26:0 (see the “ <a href="#">Global Automatic QoS Macro</a> ” section on page 53-6)
Policed-DSCP map excess rate	As per default (see the “ <a href="#">Global Automatic QoS Macro</a> ” section on page 53-6)
Default QoS IP ACL	ip dscp 0 (as per default)

**Table 53-3 Scheduling Specific Settings (Global QoS Settings)**

Field	Value
1p1q0t rxq-ratio	80% : 20% (q1 : p1)
1p3q1t wrr	20 100 200 (q1 q2 q3)
2q2t txq-ratio	80% : 20% (q1 : q2)
2q2t wrr	100 255 (q1 q2)

**Table 53-4 CoS-to-Queue Maps and Tail/WRED Settings (Global QoS Settings)**

	2q2t	Tail (2q2t)	1q2t	Tail (1q2t)	1q4t	Tail (1q4t)	1p3q1t	WRED (1p3q1t)	1p1q0t
Q1t1	0	(100%)	0, 1, 2, 3, 4	(80%)	0	(50%)	0	(70% : 100%)	0, 1, 2, 3, 4
Q1t2		(100%)	5, 6, 7	(100%)		(60%)			
Q1t3					1, 2, 3, 4	(80%)			
Q1t4					5, 6, 7	(100%)			
Q2t1	1, 2, 3, 4	(80%)					1, 2	(70% : 100%)	5, 6, 7
Q2t2	5, 6, 7	(100%)							
Q3t1							3, 4	(70% : 90%)	
Q3							6, 7	WRED disabled	
Q4t1							5		

**Table 53-5 Scheduling Specific Settings (Global QoS Settings)**

Field	Value
1p2q2t txq-ratio	70% : 15% : 15% (q1 q2 1p)
1p2q2t wrr	50 255 (q1 q2)
1p1q8t rxq-ratio	80 20 (q1 1p)
1p2q1t txq-ratio	70% : 15% : 15% (q1 q2 1p)
1p2q1t wrr	50 255 (q1 q2)

**Table 53-6 CoS-to-Queue Maps and Tail/WRED Settings (Global QoS Settings)**

	1p2q2t	WRED	1p1q4t	Tail	1p2q1t	WRED	1p1q8t	WRED
Q1t1	0	(70% : 100%)	0	(50%)	0	(70% : 100%)	0	(40% : 70%)
Q1t2		(70% : 100%)		(60%)			1, 2	(60% : 90%) (threshold 5)
Q1t3			1,2,3,4	(80%)			3, 4	(70% : 100%) (threshold 8)
Q1t4			6,7	(100%)				
Q2t1	1, 2, 3, 4	(70% : 90%)	5		1, 2, 3, 4	(70% : 90%)	5, 6, 7	
Q2t2	6, 7	(100% : 100%)						
Q2					6, 7	WRED disabled		
Q3t1	5				5			

## Port-Specific Automatic QoS Macro

The port-specific automatic QoS macro handles all inbound QoS configuration that is specific to a particular traffic type. The support is implemented for **ciscoipphone**, **ciscosoftphone**, and **trust**. See the “[CLI Interface for Automatic QoS](#)” section on page 53-13 for the associated CLI commands.

The QoS ingress port-specific settings include port trust, default CoS, classification, and policing but do not include scheduling. The input scheduling is programmed through the global automatic QoS macro. Together with the global automatic QoS macro command, all QoS settings are configured properly for a specific QoS traffic type.

The existing QoS ACLs that are already associated with a port are removed when the ACL mappings change. The ACL names and instances are not changed.

These sections describe the port-specific automatic QoS macro:

- [Port-Specific Automatic QoS Settings—ciscoipphone](#), page 53-9
- [Port-Specific Automatic QoS Settings—ciscosoftphone](#), page 53-10
- [Port-Specific Automatic QoS Settings—trust cos](#), page 53-12
- [Port-Specific Automatic QoS Settings—trust dscp](#), page 53-13

### Port-Specific Automatic QoS Settings—ciscoipphone

Use the **ciscoipphone** keyword to set the port to trust-cos and to enable trusted boundary. Combined with the global automatic QoS command, all settings are configured on the switch to properly handle the signaling, voice bearer, and PC data entering and leaving the port.

In addition to the switch-side QoS settings that are covered by the global automatic QoS command, the phone has a few QoS features that you need to configure for proper labeling to occur. The QoS configuration information is sent to the phone through CDP from the switch. The QoS values that need to be configured are the trust setting of the “PC port” on the phone (trust or untrusted) and the CoS value that is used by the phone to remark the packets in case the port is untrusted (ext-cos).

AVVID recommends an untrusted and cos-ext value of 0. The PC traffic that enters the switch is marked with CoS 0 by the phone, the voice bearer traffic that is generated by the phone is always labeled with CoS 5, and the signaling is labeled with CoS 3.

[Table 53-7](#) lists the port-specific settings that are implemented after executing the automatic QoS **ciscoipphone** macro on a port. See the “[Port-Specific Automatic QoS—voip ciscoipphone](#)” section on page 53-21 for detailed configuration examples.

**Note**

You must enable CDP version 2 for trusted boundary to work. If CDP version 2 is not enabled, a syslog message displays. See the “[CDP Warning](#)” section on page 53-24.

**Table 53-7 Port-Specific Settings for Voice (ciscoipphone Keyword)**

Item	Value
Interface type	Port-based
Policy source—config	Local
Policy source—runtime	Local (as per default)
Trust type—config	Trust-cos
Trust type—runtime	Trust-cos
Default CoS—config	0 (as per default)
Default CoS—runtime	0 (as per default)
Trust-device	Ciscoipphone
QoS ACL attached to port	trust-cos any (if 1q4t/2q2t port, otherwise none)
QoS ACL name	ACL_IP-PHONES (if 1q4t/2q2t port, otherwise none) <sup>1, 2, 3</sup>
Trust-ext	Untrusted
Cos-ext	0

1. Only the IP QoS ACLs are applied (not IPX).
2. If the ACL\_IP-PHONES name is already in use, the name ACL\_IP-PHONESx, where x is a value from 1 to 99, will be tried sequentially. If all these names are taken, a syslog message displays.
3. ACL\_IP-PHONES acl will not be created on WS-X6148-RJ-45 and WS-X6148-RJ-21 modules.

## Port-Specific Automatic QoS Settings—ciscosoftphone

On the ports that connect to a Cisco SoftPhone, the QoS settings must be configured to trust the Layer 3 markings of the traffic that enters the port. Trusting all Layer 3 markings is a security risk because the PC users could send the nonpriority traffic with DSCP 46 and gain unauthorized performance benefits. Policing on all inbound traffic prevents the malicious users from obtaining unauthorized bandwidth from the network. Policing is accomplished by rate limiting the DSCP 46 (EF) inbound traffic to the codec rate that is used by the Cisco SoftPhone application (worst case G.722). Any traffic that exceeds this rate is marked down to the default traffic rate (DSCP 0 - BE). Signaling traffic (DSCP 24) is also policed and marked down to zero if excess signaling traffic is detected. All the other inbound traffic types are reclassified to default traffic (DSCP 0 - BE).



### Caution

You must disable trusted boundary for the Cisco SoftPhone ports.

Table 53-8 lists the port-specific settings that are implemented after executing the automatic QoS **voip ciscosoftphone** macro on a port. See the “[Port-Specific Automatic QoS—voip ciscosoftphone](#)” section on page 53-22 for detailed configuration examples.

**Table 53-8 Port-Specific Settings for Voice (ciscosoftphone Keyword)**

Item	Value
Interface type	Port-based
Policy source—config	Local
Policy source—runtime	Local

**Table 53-8 Port-Specific Settings for Voice (ciscosoftphone Keyword) (continued)**

Trust type—config	untrusted
<b>Item</b>	<b>Value</b>
Trust type—runtime	untrusted
Default CoS—config	0
Default CoS—runtime	0
Trust-device	none
Trust-ext	Untrusted
Cos-ext	0
QoS ACL attached to port	trust-dscp aggregate POLICE_SOFTPHONE-DSCP46-x-y any dscp-field 46 <sup>1, 2</sup> trust-dscp aggregate POLICE_SOFTPHONE-DSCP24-x-y any dscp-field 24 *
QoS ACL name	ACL_IP-SOFTPHONES-x-y <sup>3, 4</sup>
QoS policers	aggregate POLICE_SOFTPHONE-DSCP46-3-1 rate 320 burst 20 policed-dscp aggregate POLICE_SOFTPHONE-DSCP24-3-1 rate 32 burst 8 policed-dscp
QoS policer names	POLICE_SOFTPHONE-DSCP46-x-y POLICE_SOFTPHONE-DSCP24-x-y

1. x = module number (interface on which the port-based automatic QoS macro is applied).
2. y = port number (if a range is specified, use the first number in the range).
3. Only the IP QoS ACLs are applied (not IPX).
4. If the ACL\_IP-SOFTPHONE-x-y name is already in use, the name ACL\_IP-SOFTPHONE-x-y-z, where z is a value from 1 to 99, will be tried sequentially. If all these names are taken, an error message displays. A similar action is taken with the policer name (see the “Out of Policer Names” section on page 53-24).

### Policing Configuration for ciscosoftphone

Two rate limiters are associated with the interface on which the **ciscosoftphone** port-based automatic QoS macro is executed. The two rate limiters ensure that all inbound traffic on a Cisco SoftPhone port has the following characteristics:

1. The rate of DCSP 46 is at or less than that of the expected SoftPhone application rate (G.722 – worst case).
2. The rate of DSCP 24 is at or less than the expected signaling rate.
3. All other traffic is remarked to DSCP 0 (default traffic).

Action 3 is accomplished by the default QoS ACL. Any traffic that exceeds actions (1) or (2) is policed-dscp back to zero (remarked back to DSCP 0 - BE).

DSCP 46 is policed at the rate of 320 kbps with a burst of 20 kb. DSCP 24 is policed at 32 kbps with a burst of 8 kb. The burst and rate values are based on worst-case G.722 codec with a 256-kbps maximum packet length of 256 bytes and minor signaling with a maximum packet length of 1000 bytes. Signaling is transmitted with DSCP 24 and the bearer channel of the SoftPhone stream with DSCP 46.

The port is set to untrusted for all port types to prevent ingress QoS scheduling. The global automatic QoS macro configures the policed-dscp-map to make sure that DSCP 46 is marked down to DSCP 0 and that DSCP 24 is marked down to DSCP 0. The global automatic QoS macro configures the default QoS IP ACL that is used to remark all the other traffic to DSCP 0.

### Limitations for ciscosoftphone

Because there is a limit on the total number of policers and QoS ACLs that are supported on the Catalyst 6500 series switches, similar limitations are associated with the **ciscosoftphone** automatic QoS macro. Up to 1023 aggregate policers are supported. Approximately 500 Cisco SoftPhone interfaces are supported (less interfaces are supported when other QoS ACLs and security ACLs are configured).

With a large number of Cisco SoftPhone interfaces, both the bootup time and NVRAM space could be affected. The bootup time increases with a large number of Cisco SoftPhone instances. It is possible to run out of NVRAM space with a high number of Cisco SoftPhone instances. To avoid running out of NVRAM space, you might need to use the text configuration mode. For more information, see the [“Out of TCAM Space”](#) section on page 53-23.

### Port-Specific Automatic QoS Settings—trust cos

Use the **trust cos** automatic QoS keyword for the ports that require a “trust all” solution. Use the keyword only on the ports that connect other switches or known servers because the port trusts all inbound traffic marking in Layer 2 (CoS). Trusted boundary is disabled, and no QoS policing is configured on these types of ports.

[Table 53-9](#) outlines the details of the configuration after executing the automatic QoS trust macro on a port. See the [“Port-Specific Automatic QoS—trust cos”](#) section on page 53-22 for configuration examples.

**Table 53-9** Port-Specific Settings for Trust (trust cos Keyword)

Item	Value
Interface type	Port-based
Policy source—config	Local
Policy source—runtime	Local (as per default)
Trust type—config	Trust-cos
Trust type—runtime	Trust-cos
Default CoS—config	0 (as per default)
Default CoS—runtime	0 (as per default)
Trust-device	None
QoS ACL attached to port	trust-cos any (if 1q4t/2q2t port, otherwise none)
QoS ACL name	ACL_IP-TRUSTCOS (if 1q4t/2q2t port, otherwise none) <sup>1, 2</sup>
Trust-ext	Untrusted
Cos-ext	0

1. Only the IP QoS ACLs are applied (not IPX).
2. If the ACL\_IP- TRUSTCOS name is already in use, the name ACL\_IP- TRUSTCOS<sub>x</sub>, where *x* is a value from 1 to 99, will be tried sequentially. If all these names are taken, a syslog message is displayed.

## Port-Specific Automatic QoS Settings—trust dscp

Use the **trust dscp** automatic QoS keyword for the ports that require a “trust all” type of solution. Use this keyword only on the ports that connect to the other switches or known servers because the port will be trusting all inbound traffic marking Layer 3 (DSCP). Trusted boundary is disabled, and no QoS policing is configured on these types of ports.

[Table 53-10](#) outlines the details of the configuration after executing the automatic QoS trust macro on a port. See the “[Port-Specific Automatic QoS Settings—trust dscp](#)” section on [page 53-13](#) for configuration examples.

**Table 53-10** Port Specific Settings for Trusts (*trust dscp* Keyword)

Item	Value
Interface type	Port-based
Policy source—config	Local
Policy source—runtime	Local (as per default)
Trust type—config	Trust-dscp (all except 1q4t/2q2t ports) Untrusted (1q4t/2q2t ports)
Trust type—runtime	Trust-dscp (all except 1q4t/2q2t ports) Untrusted (1q4t/2q2t ports)
Default CoS—config	0 (as per default)
Default CoS—runtime	0 (as per default)
Trust-device	None
QoS ACL attached to port	trust-dscp any (if 1q4t/2q2t port, otherwise none)
QoS ACL name	ACL_IP-TRUSTDSCP (if 1q4t/2q2t port, otherwise none) <sup>1, 2</sup>
Trust-ext	Untrusted
Cos-ext	0

1. Only the IP QoS ACLs are applied (not IPX).

2. If the ACL\_IP-TRUSTDSCP name is already in use, the name ACL\_IP-TRUSTDSCP*x*, where *x* is a value from 1 to 99, will be tried sequentially. If all these names are taken, a syslog message is displayed.

## CLI Interface for Automatic QoS

These sections describe the CLI interface for automatic QoS:

- [Global Automatic QoS Macro—set qos autoqos](#), [page 53-14](#)
- [Port-Specific Automatic QoS Macro—set port qos autoqos](#), [page 53-14](#)
- [Displaying the QoS Settings](#), [page 53-14](#)
- [Clearing the Automatic QoS Settings](#), [page 53-15](#)
- [Tracking the QoS Configuration](#), [page 53-17](#)

## Global Automatic QoS Macro—set qos autoqos

When you execute the global automatic QoS macro, all the global QoS settings are applied to all ports in the switch. After completion, a prompt displays showing the CLI for the port-based automatic QoS commands that are currently supported.

```
Console> (enable) set qos autoqos ?
Usage: set qos autoqos
Console> (enable) set qos autoqos
QoS is enabled.
.....
All ingress and egress QoS scheduling parameters configured on all ports.
CoS to DSCP, DSCP to COS, IP Precedence to DSCP and policed dscp maps configured.
Global QoS configured, port specific autoqos recommended:
    set port qos <mod/port> autoqos trust <cos|dscp>
    set port qos <mod/port> autoqos voip <ciscoipphone|ciscosoftphone>
Console> (enable)
```

## Port-Specific Automatic QoS Macro—set port qos autoqos

The port-specific automatic QoS macro accepts a *mod/port* combination and must include an AVVID-type keyword. The **ciscoipphone**, **ciscosoftphone**, and **trust** keywords are supported.

This example shows how to use the **ciscoipphone** keyword:

```
Console> (enable) set port qos 3/1 autoqos help
Usage: set port qos <mod/port> autoqos trust <cos|dscp>
       set port qos <mod/port> autoqos voip <ciscoipphone|ciscosoftphone>
Console> (enable) set port qos 3/1 autoqos voip ciscoipphone
Port 3/1 ingress QoS configured for Cisco IP Phone.
It is recommended to execute the "set qos autoqos" global command if not executed
previously.
Console> (enable)
```

This example shows how to use the **ciscosoftphone** keyword:

```
Console> (enable) set port qos 3/1 autoqos voip ciscosoftphone
Port 3/1 ingress QoS configured for Cisco Softphone.
It is recommended to execute the "set qos autoqos" global command if not executed
previously.
Console> (enable)
```

This example shows how to use the **trust cos** keyword:

```
Console> (enable) set port qos 3/1 autoqos trust cos
Port 3/1 QoS configured to trust all incoming CoS marking.
It is recommended to execute the "set qos autoqos" global command if not executed
previously.
Console> (enable)
```

This example shows how to use the **trust dscp** keyword:

```
Console> (enable) set port qos 3/1 autoqos trust dscp
Port 3/1 QoS configured to trust all incoming DSCP marking.
It is recommended to execute the "set qos autoqos" global command if not executed
previously.
Console> (enable)
```

## Displaying the QoS Settings

Enter the existing QoS **show** commands to display the QoS settings. These commands include the **show port qos** and **show qos info runtime** commands.

## Clearing the Automatic QoS Settings

You can clear the automatic QoS configuration by entering a port-based **clear** command and a global **clear** command. To clear the automatic QoS configuration, clear each interface on which automatic QoS has run with the port-based **clear** command and then enter the global **clear** command as described in the following sections:

- [Clearing the Automatic QoS Port-Based Settings, page 53-15](#)
- [Clearing the Automatic QoS Global Settings, page 53-15](#)

### Clearing the Automatic QoS Port-Based Settings

All automatic QoS settings that are configured through the port-based automatic QoS command can be configured back to the factory-default settings by entering the **clear port qos mod/port autoqos** command, as follows:

```

Console> (enable) set port qos 3/1 autoqos voip ciscosoftphone
Port 3/1 ingress QoS configured for Cisco Softphone.
It is recommended to execute the "set qos autoqos" global command if not executed
previously.
Console> (enable) clear port qos ?
  <mod/port>                Module number and Port number(s)
Console> (enable) clear port qos 3/1 ?
  autoqos                   Clear port based autoqos settings
  cos                       Clear QoS default CoS value on ports
  cos-ext                   Clear QoS default CoS extension on ports
Console> (enable) clear port qos 3/1 autoqos
Port based QoS settings will be restored back to factory defaults for port 3/1.
Do you want to continue (y/n) [n]? y
Port 3/1 autoqos settings have been cleared.
It is recommended to execute the "clear qos autoqos" global command if
not executed previously to clear global autoqos settings.
Console> (enable)

```

The port-based **clear** command is supported on all ports that support the port-based automatic QoS **set** commands. All QoS settings that are configured through the automatic QoS port-based command revert back to the factory-default settings (with the exception of automatic QoS ACLs). All QoS ACLs that are mapped to the port are unmapped from the port, even if the QoS ACL is not related to automatic QoS. The QoS ACLs that are created for automatic QoS purposes are cleared when you enter the global **clear** command.

### Clearing the Automatic QoS Global Settings

All QoS settings that are configured through the global automatic QoS command can be configured back to the factory-default settings by entering the **clear qos autoqos** command, as follows:

```

Console> (enable) clear qos autoqos
Its highly recommended to execute clear port autoqos commands prior
to the global clear command:
  clear port qos <mod/port> autoqos

Do you want to continue (y/n) [n]? y
.....
Autoqos ACL 'ACL_IP-SOFTPHONE-3-1' successfully deleted.
Cleared Autoqos policer 'POLICE_SOFTPHONE-DSCP46-3-1'
Cleared Autoqos policer 'POLICE_SOFTPHONE-DSCP24-3-1'

```

```
All ingress and egress QoS scheduling parameters set to factory default.
CoS to DSCP, DSCP to COS, IP Precedence to DSCP and policed dscp maps
configured. Global Autoqos QoS cleared.
Console> (enable)
```

The QoS ACLs that are created through the **set port autoqos** commands are cleared when you enter the global automatic QoS **clear** command. In addition, any policers that are used by the automatic QoS ACLs are cleared.

The global automatic QoS **clear** command searches for the automatic QoS ACL names. The search algorithm looks for names that begin with these strings:

- ACL\_IP-PHONES (for ciscoipphone)
- ACL\_IP-SOFTPHONE (for ciscosoftphone)
- ACL\_IP-TRUSTCOS (for trust cos)
- ACL\_IP-TRUSTDSCP (for trust dscp)

Any QoS ACL that starts with the above strings is considered an automatic QoS ACL and is cleared. If one is found and the QoS ACL is committed and not mapped to a port or a VLAN, the automatic QoS ACL is deleted.

Similarly, the search algorithm looks for the aggregate QoS policers starting with the name: POLICE\_SOFTPHONE-DSCP (for ciscosoftphone).

The global **clear** command searches for the aggregate policer names that begin with POLICE\_SOFTPHONE-DSCP. If a policer is found, and there is no QoS ACL that is associated with it, it is deleted. If a policer is found, and there is a QoS ACL that is associated with it, a warning is displayed indicating that the policer is still in use.

Various error conditions can occur when you use the global **clear** command. If you have properly executed the port-based **clear** commands before entering the global **clear** command, no error conditions should occur. However, if you execute the global **clear** command first or modify the automatic QoS configuration, these error conditions could occur:

- The automatic QoS ACLs are still mapped to a port or VLAN.

The global **clear** command does not clear the automatic QoS ACLs that are still mapped to a VLAN or port. Instead, the command displays a warning indicating the name of the QoS ACL that is still mapped to a port/VLAN.

- The aggregate policers are still in use.

If the automatic QoS policers are still in use (referenced by a QoS ACL), the global **clear** command does not remove them. Instead, it displays the name of the aggregate policer.

- The automatic QoS ACLs are uncommitted.

The global **clear** command removes only the committed automatic QoS ACLs but ignores the uncommitted automatic QoS ACLs.

This example shows what is displayed under these various error conditions:

```
Console> (enable) clear qos autoqos
Its highly recommended to execute clear port autoqos commands prior
to the global clear command:
  clear port qos <mod/port> autoqos
```

```

Do you want to continue (y/n) [n]? y
.....
Autoqos ACL 'ACL_IP-SOFTPHONE-3-2' successfully deleted.
Autoqos ACL 'ACL_IP-SOFTPHONE-3-3' successfully deleted.
Autoqos ACL 'ACL_IP-SOFTPHONE-3-4' still mapped to port or vlan.
Autoqos ACL 'ACL_IP-SOFTPHONE-3-5' still mapped to port or vlan.
Autoqos ACL 'ACL_IP-SOFTPHONE-3-6' still mapped to port or vlan.
Cleared Autoqos policer 'POLICE_SOFTPHONE-DSCP46-3-2'
Cleared Autoqos policer 'POLICE_SOFTPHONE-DSCP24-3-2'
Cleared Autoqos policer 'POLICE_SOFTPHONE-DSCP46-3-3'
Cleared Autoqos policer 'POLICE_SOFTPHONE-DSCP24-3-3'
Could not clear Autoqos policer 'POLICE_SOFTPHONE-DSCP46-3-4', still in use.
QoS is disabled.

All ingress and egress QoS scheduling parameters set to factory default.
CoS to DSCP, DSCP to COS, IP Precedence to DSCP and policed dscp maps
configured. Global Autoqos QoS cleared.
Console> (enable)

```

## Tracking the QoS Configuration

A configuration “comment” appears in the configuration file to help you determine where the QoS configuration originated: Traditional QoS or automatic QoS. The comment is created after you enter the global **set qos autoqos** command and remains in the configuration file until you enter either the **clear global autoqos** command or the **clear qos config** command. An example is as follows:

```

Console> (enable) set qos autoqos
.....
All ingress and egress QoS scheduling parameters configured on all ports.
CoS to DSCP, DSCP to COS, IP Precedence to DSCP and policed dscp maps
configured. Global QoS configured, port specific autoqos recommended:
    set port qos <mod/port> autoqos trust <cos|dscp>
    set port qos <mod/port> autoqos voip <ciscoipphone|ciscosoftphone>
Console> (enable) show config
This command shows non-default configurations only.
Use 'show config all' to show both default and non-default configurations.
.....

.....

.....

..

begin
<snip>
#qos - qos configuration via autoqos
set qos enable
set qos map 2q2t tx 2 1 cos 1
set qos map 2q2t tx 2 1 cos 2
<snip>
Console> (enable) clear qos autoqos
Its highly recommended to execute clear port autoqos commands prior
to the global clear command:
    clear port qos <mod/port> autoqos

Do you want to continue (y/n) [n]? y
.....

No Autoqos ACLs found.
No Autoqos aggregate policer(s) found.

```

QoS is disabled.

All ingress and egress QoS scheduling parameters set to factory default.  
CoS to DSCP, DSCP to COS, IP Precedence to DSCP and policed dscp maps  
configured. Global Autoqos QoS cleared.

Console> (enable) **show config**

This command shows non-default configurations only.

Use 'show config all' to show both default and non-default configurations.

.....

<snip>

#qos

<snip>

Console> (enable)

## Detailed Automatic QoS Configuration Statements

These sections provide the detailed automatic QoS configuration statements:

- [Global Automatic QoS Macro, page 53-18](#)
- [Port-Specific Automatic QoS—voip ciscoipphone, page 53-21](#)
- [Port-Specific Automatic QoS—voip ciscosoftphone, page 53-22](#)
- [Port-Specific Automatic QoS—trust cos, page 53-22](#)
- [Port-Specific Automatic QoS—trust dscp, page 53-22](#)

## Global Automatic QoS Macro

Entering the global automatic QoS command results in the following configuration:

```
set qos autoqos
-----
set qos enable

set qos policy-source local
set qos ipprec-dscp-map 0 10 18 26 34 46 48 56
set qos cos-dscp-map 0 10 18 26 34 46 48 56
set qos dscp-cos-map 0-7:0 8-15:1 16-23:2 24-31:3 32-39:4 40-47:5 48-55:6 56-63:7
set qos acl default-action ip dscp 0
set qos map 2q2t tx queue 2 2 cos 5,6,7
set qos map 2q2t tx queue 2 1 cos 1,2,3,4
set qos map 2q2t tx queue 1 1 cos 0
set qos drop-threshold 2q2t tx queue 1 100 100
set qos drop-threshold 2q2t tx queue 2 80 100
set qos drop-threshold 1q4t rx queue 1 50 60 80 100
set qos txq-ratio 2q2t 80 20
set qos wrr 2q2t 100 255

set qos map 1p3q1t tx 1 1 cos 0
set qos map 1p3q1t tx 2 1 cos 1,2
set qos map 1p3q1t tx 3 1 cos 3,4
set qos map 1p3q1t tx 3 0 cos 6,7
set qos map 1p3q1t tx 4 cos 5
set qos wrr 1p3q1t 20 100 200
set qos wred 1p3q1t queue 1 70:100
set qos wred 1p3q1t queue 2 70:100
set qos wred 1p3q1t queue 3 70:90
set qos map 1p1q0t rx 1 cos 0,1,2,3,4
set qos map 1p1q0t rx 2 cos 5,6,7
```

```
set qos rxq-ratio 1p1q0t 80 20
set qos map 1p2q2t tx 1 2 cos 0
set qos map 1p2q2t tx 2 1 cos 1,2,3,4
set qos map 1p2q2t tx 2 2 cos 6,7
set qos map 1p2q2t tx 3 cos 5
set qos txq-ratio 1p2q2t 75 15 15
set qos wrr 1p2q2t 50 255
set qos wred 1p2q2t queue 1 1 40:70
set qos wred 1p2q2t queue 1 2 70:100
set qos wred 1p2q2t queue 2 1 40:70
set qos wred 1p2q2t queue 2 2 70:100
set qos map 1p1q4t rx 1 1 cos 0
set qos map 1p1q4t rx 1 3 cos 1,2,3,4
set qos map 1p1q4t rx 1 4 cos 6,7
set qos map 1p1q4t rx 2 cos 5
set qos drop-threshold 1p1q4t rx queue 1 50 60 80 100

set qos map 1p2q1t tx 1 1 cos 0
set qos map 1p2q1t tx 2 1 cos 1,2,3,4
set qos map 1p2q1t tx 2 cos 6,7
set qos map 1p2q1t tx 3 cos 5
set qos txq-ratio 1p2q1t 75 15 15
set qos wrr 1p2q1t 50 255
set qos wred 1p2q1t queue 1 70:100
set qos wred 1p2q1t queue 2 70:100
set qos map 1p1q8t rx 1 1 cos 0
set qos map 1p1q8t rx 1 5 cos 1,2
set qos map 1p1q8t rx 1 8 cos 3,4
set qos map 1p1q8t rx 2 cos 5,6,7
set qos wred 1p1q8t queue 1 1 40:70
set qos wred 1p1q8t queue 1 5 60:90
set qos wred 1p1q8t queue 1 8 70:100
set qos rxq-ratio 1p1q8t 80 20
set qos policed-dscp-map 0:0
set qos policed-dscp-map 1:1
set qos policed-dscp-map 2:2
set qos policed-dscp-map 3:3
set qos policed-dscp-map 4:4
set qos policed-dscp-map 5:5
set qos policed-dscp-map 6:6
set qos policed-dscp-map 7:7
set qos policed-dscp-map 8:8
set qos policed-dscp-map 9:9
set qos policed-dscp-map 10:10
set qos policed-dscp-map 11:11
set qos policed-dscp-map 12:12
set qos policed-dscp-map 13:13
set qos policed-dscp-map 14:14
set qos policed-dscp-map 15:15
set qos policed-dscp-map 16:16
set qos policed-dscp-map 17:17
set qos policed-dscp-map 18:18
set qos policed-dscp-map 19:19
set qos policed-dscp-map 20:20
set qos policed-dscp-map 21:21
set qos policed-dscp-map 22:22
set qos policed-dscp-map 23:23
set qos policed-dscp-map 24:24
set qos policed-dscp-map 25:25
set qos policed-dscp-map 26:0
set qos policed-dscp-map 27:27
set qos policed-dscp-map 28:28
set qos policed-dscp-map 29:29
set qos policed-dscp-map 30:30
```

```
set qos policed-dscp-map 31:31
set qos policed-dscp-map 32:32
set qos policed-dscp-map 33:33
set qos policed-dscp-map 34:34
set qos policed-dscp-map 35:35
set qos policed-dscp-map 36:36
set qos policed-dscp-map 37:37
set qos policed-dscp-map 38:38
set qos policed-dscp-map 39:39
set qos policed-dscp-map 40:40
set qos policed-dscp-map 41:41
set qos policed-dscp-map 42:42
set qos policed-dscp-map 43:43
set qos policed-dscp-map 44:44
set qos policed-dscp-map 45:45
set qos policed-dscp-map 46:0
set qos policed-dscp-map 47:47
set qos policed-dscp-map 48:48
set qos policed-dscp-map 49:49
set qos policed-dscp-map 50:50
set qos policed-dscp-map 51:51
set qos policed-dscp-map 52:52
set qos policed-dscp-map 53:53
set qos policed-dscp-map 54:54
set qos policed-dscp-map 55:55
set qos policed-dscp-map 56:56
set qos policed-dscp-map 57:57
set qos policed-dscp-map 58:58
set qos policed-dscp-map 59:59
set qos policed-dscp-map 60:60
set qos policed-dscp-map 61:61
set qos policed-dscp-map 62:62
set qos policed-dscp-map 63:63
set qos policed-dscp-map excess-rate 0:0
set qos policed-dscp-map excess-rate 1:1
set qos policed-dscp-map excess-rate 2:2
set qos policed-dscp-map excess-rate 3:3
set qos policed-dscp-map excess-rate 4:4
set qos policed-dscp-map excess-rate 5:5
set qos policed-dscp-map excess-rate 6:6
set qos policed-dscp-map excess-rate 7:7
set qos policed-dscp-map excess-rate 8:8
set qos policed-dscp-map excess-rate 9:9
set qos policed-dscp-map excess-rate 10:10
set qos policed-dscp-map excess-rate 11:11
set qos policed-dscp-map excess-rate 12:12
set qos policed-dscp-map excess-rate 13:13
set qos policed-dscp-map excess-rate 14:14
set qos policed-dscp-map excess-rate 15:15
set qos policed-dscp-map excess-rate 16:16
set qos policed-dscp-map excess-rate 17:17
set qos policed-dscp-map excess-rate 18:18
set qos policed-dscp-map excess-rate 19:19
set qos policed-dscp-map excess-rate 20:20
set qos policed-dscp-map excess-rate 21:21
set qos policed-dscp-map excess-rate 22:22
set qos policed-dscp-map excess-rate 23:23
set qos policed-dscp-map excess-rate 24:24
set qos policed-dscp-map excess-rate 25:25
set qos policed-dscp-map excess-rate 26:26
set qos policed-dscp-map excess-rate 27:27
set qos policed-dscp-map excess-rate 28:28
set qos policed-dscp-map excess-rate 29:29
set qos policed-dscp-map excess-rate 30:30
```

```

set qos policed-dscp-map excess-rate 31:31
set qos policed-dscp-map excess-rate 32:32
set qos policed-dscp-map excess-rate 33:33
set qos policed-dscp-map excess-rate 34:34
set qos policed-dscp-map excess-rate 35:35
set qos policed-dscp-map excess-rate 36:36
set qos policed-dscp-map excess-rate 37:37
set qos policed-dscp-map excess-rate 38:38
set qos policed-dscp-map excess-rate 39:39
set qos policed-dscp-map excess-rate 40:40
set qos policed-dscp-map excess-rate 41:41
set qos policed-dscp-map excess-rate 42:42
set qos policed-dscp-map excess-rate 43:43
set qos policed-dscp-map excess-rate 44:44
set qos policed-dscp-map excess-rate 45:45
set qos policed-dscp-map excess-rate 46:46
set qos policed-dscp-map excess-rate 47:47
set qos policed-dscp-map excess-rate 48:48
set qos policed-dscp-map excess-rate 49:49
set qos policed-dscp-map excess-rate 50:50
set qos policed-dscp-map excess-rate 51:51
set qos policed-dscp-map excess-rate 52:52
set qos policed-dscp-map excess-rate 53:53
set qos policed-dscp-map excess-rate 54:54
set qos policed-dscp-map excess-rate 55:55
set qos policed-dscp-map excess-rate 56:56
set qos policed-dscp-map excess-rate 57:57
set qos policed-dscp-map excess-rate 58:58
set qos policed-dscp-map excess-rate 59:59
set qos policed-dscp-map excess-rate 60:60
set qos policed-dscp-map excess-rate 61:61
set qos policed-dscp-map excess-rate 62:62
set qos policed-dscp-map excess-rate 63:63

```

## Port-Specific Automatic QoS—voip ciscoipphone

Entering the port-specific automatic QoS command results in the following configuration:

```

set port qos mod/port autoqos voip ciscoipphone
-----
set port qos mod/port policy-source local
set port qos mod/port port-based
set port qos mod/port cos 0
set port qos mod/port cos-ext 0
set port qos mod/port trust-ext untrusted
set port qos mod/port trust-device ciscoipphone

```

If the port type is 1q4t/2q2t, the configuration is as follows:

```

set qos acl ip ACL_IP-PHONES trust-cos any
commit qos acl ACL_IP-PHONES
set qos acl map ACL_IP-PHONES mode/port
set port qos mod/port trust trust-cos

```

If the port type is another port type, the configuration is as follows:

```

set port qos mod/port trust trust-cos

```



### Note

If the ACL\_IP-PHONES name is in use, automatic QoS checks if the existing ACL is the same as the one that is trying to be created. If the existing QoS ACL is the same, automatic QoS reuses it. If the existing QoS ACL is not the same, automatic QoS attempts other names.

## Port-Specific Automatic QoS—voip ciscosoftphone

Entering the port-specific automatic QoS command results in the following configuration:

```

set port qos mod/port autoqos voip ciscosoftphone
-----
set port qos mod/port policy-source local
set port qos mod/port port-based
set port qos mod/port cos 0
set port qos mod/port cos-ext 0
set port qos mod/port trust-ext untrusted
set port qos mod/port trust-device none
set port qos mod/port trust untrusted
set qos policer aggregate POLICE_SOFTPHONE-DSCP46-mod-port rate 320 burst 20 policed-dscp
set qos policer aggregate POLICE_SOFTPHONE-DSCP26-mod-port rate 32 burst 8 policed-dscp
set qos acl ip ACL_IP-SOFTPHONE-mod-port trust-dscp aggregate
POLICE_SOFTPHONE-DSCP46-mod-port any dscp-field 46
set qos acl ip ACL_IP-SOFTPHONE-mod-port trust-dscp aggregate
POLICE_SOFTPHONE-DSCP26-mod-port any dscp-field 26
commit qos acl ACL_IP-SOFTPHONE-mod-port
set qos acl map ACL_IP-SOFTPHONE-mod-port mod/port

```

## Port-Specific Automatic QoS—trust cos

Entering the port-specific automatic QoS command results in the following configuration:

```

set port qos mod/port autoqos trust cos
-----
set port qos mod/port policy-source local
set port qos mod/port port-based
set port qos mod/port cos 0
set port qos mod/port cos-ext 0
set port qos mod/port trust-ext untrusted
set port qos mod/port trust-device none

```

If the port type is 1q4t/2q2t, the configuration is as follows:

```

set qos acl ip ACL_IP-TRUSTCOS trust-cos any
commit qos acl ACL_IP-TRUSTCOS
set qos acl map ACL_IP-TRUSTCOS mode/port
set port qos mod/port trust trust-cos

```

If the port type is another port type, the configuration is as follows:

```

set port qos mod/port trust trust-cos

```

## Port-Specific Automatic QoS—trust dscp

Entering the port-specific automatic QoS command results in the following configuration:

```

set port qos mod/port autoqos trust dscp
-----
set port qos mod/port policy-source local
set port qos mod/port port-based
set port qos mod/port cos 0
set port qos mod/port cos-ext 0
set port qos mod/port trust-ext untrusted
set port qos mod/port trust-device none

```

If the port type is 1q4t/2q2t, the configuration is as follows:

```
set qos acl ip ACL_IP-TRUSTDSCP trust-dscp any
commit qos acl ACL_IP-TRUSTDSCP
set qos acl map ACL_IP-TRUSTDSCP mode/port
set port qos mod/port trust untrusted
```

If the port type is another port type, the configuration is as follows:

```
set port qos mod/port trust trust-dscp
```

## Warning and Error Conditions

These sections describe the warnings and error conditions for automatic QoS:

- [Out of ACL Names, page 53-23](#)
- [Out of TCAM Space, page 53-23](#)
- [COPS Warning Message, page 53-24](#)
- [CDP Warning, page 53-24](#)
- [Out of Policer Names, page 53-24](#)
- [QoS Disabled, page 53-25](#)

### Out of ACL Names

When creating a QoS ACL for a 1q4t/2q2t type port to fix the trust problem, you may note that the following QoS ACL names are already in use (where x=1 to 99):

- ACL\_IP-PHONESx (for **ciscoipphone**)
- ACL\_IP-SOFTPHONE-m-p-x (for **ciscosoftphone**)
- ACL\_IP-TRUSTCOSx (for **trust cos**)
- ACL\_IP-TRUSTDSCPx (for **trust dscp**)

This example shows the display when the system is out of ACL names:

```
Console> (enable) set port qos 4/1 autoqos voip ciscoipphone
ERROR: IP QoS ACL name in use, could not configure QoS ACL.
Rename existing QoS ACL ACL_IP-PHONES.
Autoqos did not complete. Settings remain unchanged.
Console> (enable)
```

### Out of TCAM Space

When configuring the ACLs using the port-based automatic QoS command, it is possible to have a full TCAM. In this event, an error message displays and the port-based automatic QoS command fails, leaving all QoS settings unchanged.

This example shows the display when the system is out of TCAM space:

```
Console> (enable) set port qos 4/1 autoqos voip ciscoipphone
Error: Please remove QoS or security ACLs to make space for new QoS ACL.
Autoqos did not complete. Settings remain unchanged.
Console> (enable)
```

## COPS Warning Message

If COPS has been enabled globally or enabled on a port, executing the global automatic QoS command or the port-specific automatic QoS command changes the policy source to local and a warning message displays.

This example shows that if the port-based command is successful, the port-based policy setting is changed to local as follows:

```
Console> (enable) set port qos 4/1 autoqos voip ciscosoftphone
Warning:  QoS policy changed to local for port 4/1.
Port 4/1 ingress QoS configured for ciscosoftphone.
It is recommended to execute the "set qos autoqos" global command if not executed
previously.
```

This example for the global command shows that if the global QoS policy is COPS before the global automatic QoS command is executed, a warning message displays as follows:

```
Console> (enable) set qos autoqos
.....
Warning:  QoS policy source changed to local.
All ingress and egress QoS scheduling parameters configured on all ports.
CoS to DSCP, DSCP to COS and IP Precedence to DSCP maps configured.
Global QoS configured, port specific autoqos recommended:
  set port qos <mod/port> autoqos trust [cos|dscp]
  set port qos <mod/port> autoqos voip [ciscoipphone|ciscosoftphone]
Console> (enable)
```

## CDP Warning

When executing the port-specific automatic QoS command with the **ciscoipphone** keyword without the trust option, the trust-device feature is enabled. The trust-device feature is dependent on CDP. If CDP is not enabled or not running version 2, a warning message displays as follows:

```
Console> (enable) set port qos 4/1 autoqos voip ciscoipphone
Warning:  CDP is disabled or CDP version 1 is in use.  Ensure that CDP version 2 is
enabled globally, and also ensure that CDP is enabled on the port(s) you wish to configure
autoqos on.
Port 4/1 ingress QoS configured for ciscoipphone.
It is recommended to execute the "set qos autoqos" global command if not executed
previously.
Console> (enable)
```

## Out of Policer Names

When executing the port-specific automatic QoS command with the **ciscosoftphone** keyword, two policer instances are created and named with the following strings:

- POLICE\_SOFTPHONE-DSCP46-x-y
- POLICE\_SOFTPHONE-DSCP26-x-y

where x is the module number and y is the port number of the *mod/port* combination that is specified with the **ciscosoftphone** keyword.

If the above policer names are already in use, the macro attempts the following names:

- POLICE\_SOFTPHONE-DSCP46-x-y-z
- POLICE\_SOFTPHONE-DSCP26-x-y-z

where z = 1 to 99 starting from 1. Both names must pass with the same z value or the macro attempts the next z value until both names are valid with the same z value. If the z = 99 attempt fails, this error message displays and all settings remain unchanged:

```
Console> (enable) set port qos 4/1 autoqos voip ciscosoftphone
ERROR: QoS policer name in use, could not configure QoS policer.
Rename existing QoS policer POLICE_SOFTPHONE-DSCP46-4-1 and/or
POLICE_SOFTPHONE-DSCP26-4-1.
Autoqos did not complete. Settings remain unchanged.
Console> (enable)
```

## QoS Disabled

When executing any port-based automatic QoS command on an interface where QoS is disabled, a notification message appears in the CLI as follows:

```
Console> (enable) set port qos 4/1 autoqos voip ciscosoftphone
Port 4/1 ingress QoS configured for ciscosoftphone. Policing configured on 4/1.
QoS is disabled, changes will take effect after QoS is enabled.
It is recommended to execute the "set qos autoqos" global command if not executed
previously.
Console> (enable)
```

## syslog Additions

Set the switch logging level to 4 or 5 for the QoS facility (**set logging level qos 5**) as follows:

- Log level 4 = Warnings
- Log level 5 = Notices

These sections describe the syslog additions for the automatic QoS features:

- [CDP Warning —Warning Level, page 53-25](#)
- [Interface Change for All Ports Required—Warning Level, page 53-26](#)

## CDP Warning —Warning Level

When executing the port-based automatic QoS **voip ciscoipphone** keyword on a port where either CDP is disabled on the port or globally, or is running in version 1 mode, a warning message displays as follows:

```
Console> (enable)
2001 Jun 02 09:20:42 %QOS-4-DEVICE_CDP_DIS:Trust-Device feature enabled with CDP disabled
or running in v1 mode.
Console> (enable)
```

## Interface Change for All Ports Required—Warning Level

For the 1p1q0t/1p3q1t ports, if a change in an interface type is needed (if VLAN-based mode is configured before the automatic QoS macro is executed), a syslog message displays indicating that all ports in the module had the interface type changed to port-based QoS, as follows:

```
Console> (enable)
2001 Jun 02 09:20:42 %QOS-3-INTERFACE-CHANGED:All ports in module 3 have been configured
to port-based QoS.
Console> (enable)
```

## Other Relevant syslog Messages

These sections describe the other relevant syslog messages that relate to the automatic QoS configuration:

- [Device No Longer Detected on the Port—Notice Level \(Trusted Boundary\), page 53-26](#)
- [Device Detected on the Port—Notice Level, page 53-26](#)
- [CDP Disabled with Trust-Dev Configured—Warning Level, page 53-26](#)

## Device No Longer Detected on the Port—Notice Level (Trusted Boundary)

After enabling trusted boundary on a port (using the **ciscoipphone** keyword), if the phone is detected to have left the port, a syslog message displays stating that the device has left and the port trust state has been changed, as follows:

```
Console> (enable)
2001 Jun 02 09:20:42 %QOS-5-DEVICE_LOST:ciscoipphone not detected on port 4/1, port set to
untrusted.
Console> (enable)
```

## Device Detected on the Port—Notice Level

If the trusted device joins the port, a syslog message displays indicating the change in the port trust status. The heading contains the new trust type of the port as specified in the configuration. This example shows that the port trust for port 4/1 is set to “trust-cos” in the configuration:

```
Console> (enable)
2001 Jun 02 09:20:42 %QOS-5-DEVICE_DETECTED:ciscoipphone detected on port 4/1, port set to
trust-cos.
Console> (enable)
```

## CDP Disabled with Trust-Dev Configured—Warning Level

When executing the port-based automatic QoS **ciscoipphone** keyword on a port, the trust-device is configured to “ciscoipphone” which activates trusted boundary. After trusted boundary is enabled, if either CDP is disabled on that port or CDP is running in version 1 mode, or CDP is globally disabled, a syslog message displays as follows:

```
Console> (enable)
2001 Jun 02 09:20:42 %QOS-4-DEVICE_CDP_DIS:Trust-Device feature enabled with CDP disabled
or running in v1 mode.
Console> (enable)
```

This message is displayed only once when a problem is detected. When the problem is fixed, the message can appear again if the configuration is broken again. There is a maximum time of 15 seconds for detecting a misconfiguration.

## Summary of Automatic QoS Features

These sections summarize the automatic QoS features:

- [Global Automatic QoS Features \(set qos autoqos\)](#), page 53-27
- [Port-Based Automatic QoS Features](#), page 53-27

### Global Automatic QoS Features (set qos autoqos)

The global automatic QoS feature is summarized as follows:

- Configures all switch-wide QoS parameters to accommodate and properly prioritize all traffic types that are listed in the “[Typical CoS and DSCP Values for Voice and Video Networks](#)” section on [page 53-2](#).
- Overwrites any old or misconfigured settings that were previously applied.
- Works with the port-based automatic QoS command.

### Port-Based Automatic QoS Features

The port-based automatic QoS features are summarized as follows:

- `voip ciscoipphone`
  - Changes the port to port-based QoS.
  - For the 1p1q0t/1p3q1t ports, changes all ports to port-based mode.
  - Creates a trust-cos QoS ACL for the ports that need it (1q4t/2q2t ports).
  - Applies the trust-cos ACL to the port (1q4t/2q2t ports).
  - Enables trusted boundary on the port.
  - Sets the port trust to trust-cos.
  - Supports the ports with or without an auxiliary VLAN.
  - Supported only on the 10/100 ports and the 10/100/1000 ports.
  - PFC or PFC2 not required (PFC and PFC2 are supported).
- `voip ciscosoftphone`
  - Changes the port to port-based QoS.
  - Changes trust to untrusted.
  - For the 1p1q0t/1p3q1t ports, changes all ports to port-based mode.
  - Disables trusted boundary on the port.
  - Applies two rate limiters, one for DSCP 46 and one for DSCP 26 inbound traffic, and trusts only inbound DSCP 46 and DSCP 26 traffic.
  - Results in traffic that is marked down to DSCP 0 for violations of either rate limiter.
  - Remarks all other (non-DSCP 26 and 46) inbound traffic to DSCP 0.

- Supports the ports with or without an auxiliary VLAN.
- Supported on all ports.
- Requires the PFC or the PFC2.
- trust cos
  - Changes the port to port-based QoS.
  - For the 1p1q0t/1p3q1t ports, changes all ports to port-based mode.
  - Creates a trust-cos QoS ACL for the ports that need it (1q4t/2q2t ports).
  - Applies the trust-cos ACL to the port (1q4t/2q2t ports).
  - Disables trusted boundary on the port.
  - Sets port trust to trust-cos.
  - Supports the ports with or without an auxiliary VLAN.
  - Supported on all ports.
  - PFC not required (PFC and PFC2 are supported).
- trust dscp
  - Changes the port to port-based QoS.
  - For the 1p1q0t/1p3q1t ports, changes all ports to port-based mode.
  - Creates a trust-dscp QoS ACL for the ports that need it (1q4t/2q2t ports).
  - Applies the trust-dscp ACL to the port (1q4t/2q2t ports).
  - Disables trusted boundary on the port.
  - Sets port trust to untrusted (1q4t/2q2t ports) or trust-dscp (not on 1q4t/2q2t ports).
  - Supports the ports with or without an auxiliary VLAN.
  - Supported on all ports.
  - Requires the PFC or the PFC2.

## Using Automatic QoS in Your Network



### Tip

To ensure that automatic QoS works properly, you should execute the global automatic QoS macro and, for each interface, you should execute the interface-specific automatic QoS macro.

Depending on the interface and what is connected to it, you will need to execute different automatic QoS macros. To execute the global automatic QoS macro, and then for each interface, execute the interface-specific automatic QoS macro with the appropriate keyword, perform these steps:

- 
- Step 1** Execute the **set qos autoqos** command to enable QoS and configure all the outbound QoS settings.
  - Step 2** For each port, execute the port-based automatic QoS commands as shown in [Table 53-11](#).
-

**Table 53-11**      **Using Automatic QoS Keywords**

<b>Keyword</b>	<b>Port Type</b>
<b>ciscoipphone</b>	Ports that connect only a Cisco IP Phone 79xx.
<b>ciscoipphone</b>	Ports that connect a Cisco IP Phone 79xx with a PC connected to the 79xx.
<b>ciscoipphone</b>	Ports that connect a Cisco IP Phone 79xx with a PC connected to the 79xx running Cisco SoftPhone <sup>1</sup> .
<b>ciscosoftphone</b>	Ports that connect a PC running Cisco SoftPhone without a Cisco IP Phone 79xx.
<b>trust</b>	Ports that connect to other places in the network where all automatic QoS traffic types exist <sup>2</sup> .

1. For cases where ports connect a Cisco IP Phone 79xx with a PC running Cisco SoftPhone, the control traffic through CTI communication with the Cisco CallManager is tagged but is remarked to DSCP 0.
2. For ports connecting to other networks or Cisco CallManagers, we recommend that you use the **trust** keyword. Currently, Cisco CallManager and gateways correctly mark skinny, H.323, and MGCP signaling traffic. However, some versions of Cisco CallManager do not explicitly mark H.323 and MGCP traffic. We recommend QoS ACLs for these situations.

