CHAPTER 36

Configuring Auto-QoS

Finding Feature Information

Your software release may not support all the features documented in this chapter. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Auto-QoS

- When enabling auto-QoS with a Cisco IP phone on a routed port, you must assign a static IP address to the IP phone.
- By default, the CDP is enabled on all ports. For auto-QoS to function properly, do not disable the CDP.

Restrictions for Auto-QoS

- To use this feature, the switch must be running the LAN Base image.
- Connected devices must use Cisco Call Manager Version 4 or later.
- This release supports only Cisco IP SoftPhone Version 1.3(3) or later.
- To take advantage of the auto-QoS defaults, you should enable auto-QoS before you configure other QoS commands. If necessary, you can fine-tune the QoS configuration, but we recommend that you do so only after the auto-QoS configuration is completed. For more information, see the Effects of Auto-QoS on the Configuration, page 36-7.
- Control traffic (such as spanning-tree bridge protocol data units [BPDUs] and routing update packets) received by the switch are subject to all ingress QoS processing.
- You are likely to lose data when you change queue settings; therefore, try to make changes when traffic is at a minimum.

- Auto-QoS configures the switch for VoIP with Cisco IP phones on nonrouted and routed ports. Auto-QoS also configures the switch for VoIP with devices running the Cisco SoftPhone application.
- When a device running Cisco SoftPhone is connected to a nonrouted or routed port, the switch supports only one Cisco SoftPhone application per port.
- Auto-Qos VoIP uses the **priority-queue** interface configuration command for an egress interface. You can also configure a policy-map and trust device on the same interface for Cisco IP phones.
- 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 this new policy map instead of the generated one, remove the generated policy map from the interface, and apply the new policy map to the interface.
- You can enable auto-QoS on static, dynamic-access, voice VLAN access, and trunk ports.

Information About Auto-QoS

This chapter describes how to configure quality of service (QoS) by using automatic QoS (auto-QoS) command on the switch. With QoS, you can provide preferential treatment to certain types of traffic at the expense of others. Without QoS, the switch offers best-effort service to each packet, regardless of the packet contents or size. It sends the packets without any assurance of reliability, delay bounds, or throughput.

You can configure QoS on physical ports and on switch virtual interfaces (SVIs). Other than to apply policy maps, you configure the QoS settings, such as classification, queueing, and scheduling, the same way on physical ports and SVIs. When configuring QoS on a physical port, you apply a nonhierarchical policy map to a port. When configuring QoS on an SVI, you apply a nonhierarchical or a hierarchical policy map.

The switch supports some of the modular QoS CLI (MQC) commands. For more information about the MQC commands, see the “Modular Quality of Service Command-Line Interface Overview” chapter of the *Cisco IOS Quality of Service Solutions Guide*.

Auto-QoS

You can use the auto-QoS feature to simplify the deployment of QoS features. Auto-QoS determines the network design and enables QoS configurations so that the switch can prioritize different traffic flows. It uses the ingress and egress queues instead of using the default (disabled) QoS behavior. The switch offers best-effort service to each packet, regardless of the packet contents or size, and sends it from a single queue.

When you enable auto-QoS, it automatically classifies traffic based on the traffic type and ingress packet label. The switch uses the classification results to choose the appropriate egress queue.

Auto-QoS supports IPv4 and IPv6 traffic when you configure the dual IPv4 and IPv6 SDM template with the **sdm prefer dual ipv4-and-ipv6** global configuration command.

You use auto-QoS commands to identify ports connected to Cisco IP phones and to devices running the Cisco SoftPhone application. You also use the commands to identify ports that receive trusted traffic through an uplink. Auto-QoS then performs these functions:

- Detects the presence or absence of Cisco IP phones
- Configures QoS classification

- Configures egress queues

Generated Auto-QoS Configuration

By default, auto-QoS is disabled on all ports.

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 as shown in Table 36-1.

Table 36-1 Traffic Types, Packet Labels, and Queues

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

1. VoIP = voice over IP

Table 36-2 shows the generated auto-QoS configuration for the ingress queues.

Table 36-2 Auto-QoS Configuration for the Ingress Queues

Ingress Queue	Queue Number	CoS-to-Queue Map	Queue Weight (Bandwidth)	Queue (Buffer) Size
SRR shared	1	0, 1	81 percent	67 percent
Priority	2	2, 3, 4, 5, 6, 7	19 percent	33 percent

Table 36-3 shows the generated auto-QoS configuration for the egress queues.

Table 36-3 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	1	5	up to100 percent	16 percent	10 percent
SRR shared	2	3, 6, 7	10 percent	6 percent	10 percent
SRR shared	3	2, 4	60 percent	17 percent	26 percent
SRR shared	4	0, 1	20 percent	61 percent	54 percent

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

- QoS is globally enabled (**mls qos** global configuration command), and other global configuration commands are added.
- When you enter the **auto qos voip cisco-phone** interface configuration command on a port at the edge of the network that is connected to a Cisco IP phone, the switch enables the trusted boundary feature. The switch uses the Cisco Discovery Protocol (CDP) to detect the presence or absence 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 switch configures ingress and egress queues on the port according to the settings in Table 36-2 and Table 36-3. 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 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. The switch configures ingress and egress queues on the port according to the settings in Table 36-2 and Table 36-3.
- When you enter the **auto qos voip trust** interface configuration command on a port connected to the interior of the network, 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). The switch configures the ingress and egress queues on the port according to the settings in Table 36-2 and Table 36-3.

  For information about the trusted boundary feature, see the "Configuring a Trusted Boundary to Ensure Port Security" section on page 35-34.

When you enable auto-QoS by using the **auto qos voip cisco-phone**, the **auto qos voip cisco-softphone**, or the **auto qos voip trust** interface configuration command, the switch automatically generates a QoS configuration based on the traffic type and ingress packet label and applies the commands listed in Table 36-4 to the port.

Table 36-4 Generated Auto-QoS Configuration

Description	Automatically Generated Command
The switch automatically enables standard QoS and configures the CoS-to-DSCP map (maps CoS values in incoming packets to a DSCP value).	`Switch(config)# mls qos` `Switch(config)# mls qos map cos-dscp 0 8 16 26 32 46 48 56`

The switch automatically maps CoS values to an ingress queue and to a threshold ID.	`Switch(config)# no mls qos srr-queue input cos-map`
	`Switch(config)# mls qos srr-queue input cos-map queue 1 threshold 3 0`
	`Switch(config)# mls qos srr-queue input cos-map queue 1 threshold 2 1`
	`Switch(config)# mls qos srr-queue input cos-map queue 2 threshold 1 2`
	`Switch(config)# mls qos srr-queue input cos-map queue 2 threshold 2 4 6 7`
	`Switch(config)# mls qos srr-queue input cos-map queue 2 threshold 3 3 5`

Table 36-4 Generated Auto-QoS Configuration (continued)

Description	Automatically Generated Command
The switch automatically maps CoS values to an egress queue and to a threshold ID.	Switch(config)# **no mls qos srr-queue output cos-map** Switch(config)# **mls qos srr-queue output cos-map queue 1 threshold 3 5** Switch(config)# **mls qos srr-queue output cos-map queue 2 threshold 3 3 6 7** Switch(config)# **mls qos srr-queue output cos-map queue 3 threshold 3 2 4** Switch(config)# **mls qos srr-queue output cos-map queue 4 threshold 2 1** Switch(config)# **mls qos srr-queue output cos-map queue 4 threshold 3 0**
The switch automatically maps DSCP values to an ingress queue and to a threshold ID.	Switch(config)# **no mls qos srr-queue input dscp-map** Switch(config)# **mls qos srr-queue input dscp-map queue 1 threshold 2 9 10 11 12 13 14 15** Switch(config)# **mls qos srr-queue input dscp-map queue 1 threshold 3 0 1 2 3 4 5 6 7** Switch(config)# **mls qos srr-queue input dscp-map queue 1 threshold 3 32** Switch(config)# **mls qos srr-queue input dscp-map queue 2 threshold 1 16 17 18 19 20 21 22 23** Switch(config)# **mls qos srr-queue input dscp-map queue 2 threshold 2 33 34 35 36 37 38 39 48** Switch(config)# **mls qos srr-queue input dscp-map queue 2 threshold 2 49 50 51 52 53 54 55 56** Switch(config)# **mls qos srr-queue input dscp-map queue 2 threshold 2 57 58 59 60 61 62 63** Switch(config)# **mls qos srr-queue input dscp-map queue 2 threshold 3 24 25 26 27 28 29 30 31** Switch(config)# **mls qos srr-queue input dscp-map queue 2 threshold 3 40 41 42 43 44 45 46 47**
The switch automatically maps DSCP values to an egress queue and to a threshold ID.	Switch(config)# **no mls qos srr-queue output dscp-map** Switch(config)# **mls qos srr-queue output dscp-map queue 1 threshold 3 40 41 42 43 44 45 46 47** Switch(config)# **mls qos srr-queue output dscp-map queue 2 threshold 3 24 25 26 27 28 29 30 31** Switch(config)# **mls qos srr-queue output dscp-map queue 2 threshold 3 48 49 50 51 52 53 54 55** Switch(config)# **mls qos srr-queue output dscp-map queue 2 threshold 3 56 57 58 59 60 61 62 63** Switch(config)# **mls qos srr-queue output dscp-map queue 3 threshold 3 16 17 18 19 20 21 22 23** Switch(config)# **mls qos srr-queue output dscp-map queue 3 threshold 3 32 33 34 35 36 37 38 39** Switch(config)# **mls qos srr-queue output dscp-map queue 4 threshold 1 8** Switch(config)# **mls qos srr-queue output dscp-map queue 4 threshold 2 9 10 11 12 13 14 15** Switch(config)# **mls qos srr-queue output dscp-map queue 4 threshold 3 0 1 2 3 4 5 6 7**

Table 36-4 Generated Auto-QoS Configuration (continued)

Description	Automatically Generated Command

The switch automatically sets up the ingress queues, with queue 2 as the priority queue and queue 1 in shared mode. The switch also configures the bandwidth and buffer size for the ingress queues.	`Switch(config)# no mls qos srr-queue input priority-queue 1`
	`Switch(config)# no mls qos srr-queue input priority-queue 2`
	`Switch(config)# mls qos srr-queue input bandwidth 90 10`
	`Switch(config)# mls qos srr-queue input threshold 1 8 16`
	`Switch(config)# mls qos srr-queue input threshold 2 34 66`
	`Switch(config)# mls qos srr-queue input buffers 67 33`

The switch automatically configures the egress queue buffer sizes. It configures the bandwidth and the SRR mode (shaped or shared) on the egress queues mapped to the port.	`Switch(config)# mls qos queue-set output 1 threshold 1 138 138 92 138`
	`Switch(config)# mls qos queue-set output 1 threshold 2 138 138 92 400`
	`Switch(config)# mls qos queue-set output 1 threshold 3 36 77 100 318`
	`Switch(config)# mls qos queue-set output 1 threshold 4 20 50 67 400`
	`Switch(config)# mls qos queue-set output 2 threshold 1 149 149 100 149`
	`Switch(config)# mls qos queue-set output 2 threshold 2 118 118 100 235`
	`Switch(config)# mls qos queue-set output 2 threshold 3 41 68 100 272`
	`Switch(config)# mls qos queue-set output 2 threshold 4 42 72 100 242`
	`Switch(config)# mls qos queue-set output 1 buffers 10 10 26 54`
	`Switch(config)# mls qos queue-set output 2 buffers 16 6 17 61`
	`Switch(config-if)# priority-que out`
	`Switch(config-if)# srr-queue bandwidth share 10 10 60 20`

If you entered the **auto qos voip trust** command, the switch automatically sets the ingress classification to trust the CoS value received in the packet on a nonrouted port by using the **mls qos trust cos** command or to trust the DSCP value received in the packet on a routed port by using the **mls qos trust dscp** command.	`Switch(config-if)# mls qos trust cos` `Switch(config-if)# mls qos trust dscp`
If you entered the **auto qos voip cisco-phone** command, the switch automatically enables the trusted boundary feature, which uses the CDP to detect the presence or absence of a Cisco IP phone.	`Switch(config-if)# mls qos trust device cisco-phone`

Table 36-4 Generated Auto-QoS Configuration (continued)

Description	Automatically Generated Command

If you entered the **auto qos voip cisco-softphone** command, the switch automatically creates class maps and policy maps.	`Switch(config)# mls qos map policed-dscp 24 26 46 to 0`
	`Switch(config)# class-map match-all AutoQoS-VoIP-RTP-Trust`
	`Switch(config-cmap)# match ip dscp ef`
	`Switch(config)# class-map match-all AutoQoS-VoIP-Control-Trust`
	`Switch(config-cmap)# match ip dscp cs3 af31`
	`Switch(config)# policy-map AutoQoS-Police-SoftPhone`
	`Switch(config-pmap)# class AutoQoS-VoIP-RTP-Trust`
	`Switch(config-pmap-c)# set dscp ef`
	`Switch(config-pmap-c)# police 320000 8000 exceed-action policed-dscp-transmit`
	`Switch(config-pmap)# class AutoQoS-VoIP-Control-Trust`
	`Switch(config-pmap-c)# set dscp cs3`
	`Switch(config-pmap-c)# police 32000 8000 exceed-action policed-dscp-transmit`

After creating the class maps and policy maps, the switch automatically applies the policy map called *AutoQoS-Police-SoftPhone* to an ingress interface on which auto-QoS with the Cisco SoftPhone feature is enabled.	`Switch(config-if)# service-policy input AutoQoS-Police-SoftPhone`

If you entered the **auto qos voip cisco-phone** command, the switch automatically creates class maps and policy maps.	`witch(config)# mls qos map policed-dscp 24 26 46 to 0`
	`Switch(config)# class-map match-all AutoQoS-VoIP-RTP-Trust`
	`Switch(config-cmap)# match ip dscp ef`
	`Switch(config)# class-map match-all AutoQoS-VoIP-Control-Trust`
	`Switch(config-cmap)# match ip dscp cs3 af31`
	`Switch(config)# policy-map AutoQoS-Police-CiscoPhone`
	`Switch(config-pmap)# class AutoQoS-VoIP-RTP-Trust`
	`Switch(config-pmap-c)# set dscp ef`
	`Switch(config-pmap-c)# police 320000 8000 exceed-action policed-dscp-transmit`
	`Switch(config-pmap)# class AutoQoS-VoIP-Control-Trust`
	`Switch(config-pmap-c)# set dscp cs3`
	`Switch(config-pmap-c)# police 32000 8000 exceed-action policed-dscp-transmit`

After creating the class maps and policy maps, the switch automatically applies the policy map named *AutoQoS-Police-CiscoPhone* to an ingress interface on which auto-QoS with the Cisco IP phone feature is enabled.	`Switch(config-if)# service-policy input AutoQoS-Police-CiscoPhone`

Effects of Auto-QoS on the Configuration

When auto-QoS is enabled, the **auto qos voip** interface configuration command and the generated configuration are added to the running configuration.

The switch applies the auto-QoS-generated commands as if the commands were entered from the 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.

To display the QoS commands that are automatically generated when auto-QoS is enabled or disabled, enter the **debug auto qos** privileged EXEC command *before* enabling auto-QoS. For more information, see the **debug autoqos** command in the command reference for this release.

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).

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

How to Configure Auto-QoS

Enabling Auto-QoS for VoIP

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**interface** *interface-id*	Specifies the port that is connected to a Cisco IP phone, the port that is connected to a device running the Cisco SoftPhone feature, or the uplink port that is connected to another trusted switch or router in the interior of the network, and enter interface configuration mode.
Step 3	**auto qos voip** {**cisco-phone** | **cisco-softphone** | **trust**}	Enables auto-QoS. • **cisco-phone**—Specifies the port is connected to a Cisco IP phone, the QoS labels of incoming packets are trusted only when the telephone is detected. • **cisco-softphone**—Specifies the port is connected to a device running the Cisco SoftPhone feature. • **trust**—Specifies the uplink port is connected to a trusted switch or router, and the VoIP traffic classification in the ingress packet is trusted.
Step 4	**end**	Returns to privileged EXEC mode.

Configuring QoS to Prioritize VoIP Traffic

This task explains how to configure the switch at the edge of the QoS domain to prioritize the VoIP traffic over all other traffic:

	Command	Purpose
Step 1	**debug auto qos**	Enables debugging for auto-QoS. When debugging is enabled, the switch displays the QoS configuration that is automatically generated when auto-QoS is enabled.
Step 2	**configure terminal**	Enters global configuration mode.
Step 3	**cdp enable**	Enable CDP globally. By default, it is enabled.
Step 4	**interface** *interface-id*	Specifies the switch port connected to the Cisco IP phone, and enters interface configuration mode.
Step 5	**auto qos voip cisco-phone**	Enables auto-QoS on the port, and specifies that the port is connected to a Cisco IP phone. The QoS labels of incoming packets are trusted only when the Cisco IP phone is detected.
Step 6	**exit**	Returns to global configuration mode.
Step 7		Repeat Steps 4 to 6 for as many ports as are connected to the Cisco IP phone.
Step 8	**interface** *interface-id*	Specifies the switch port identified as connected to a trusted switch or router, and enters interface configuration mode. See Figure 36-1.
Step 9	**auto qos voip trust**	Enables auto-QoS on the port, and specifies that the port is connected to a trusted router or switch.
Step 10	**end**	Returns to privileged EXEC mode.

Monitoring and Maintaining Auto-QoS

Command	Purpose
show auto qos [**interface** [*interface-id*]]	Displays the QoS commands entered on the interfaces on which auto-QoS is enabled.
show mls qos	Displays global QoS configuration information.
show mls qos interface [*interface-id*] [**buffers** | **queueing**]	Displays QoS information at the port level.
show mls qos maps [**cos-dscp** | **cos-input-q** | **cos-output-q** | **dscp-cos** | **dscp-input-q** | **dscp-mutation** | **dscp-output-q** | **ip-prec-dscp** | **policed-dscp**]	Displays QoS mapping information. During classification, QoS uses the mapping tables to represent the priority of the traffic and to derive a corresponding CoS or DSCP value from the received CoS, DSCP, or IP precedence value.
show mls qos input-queue	Displays QoS settings for the ingress queues.
show running-config	Displays the current operating configuration, including defined macros.

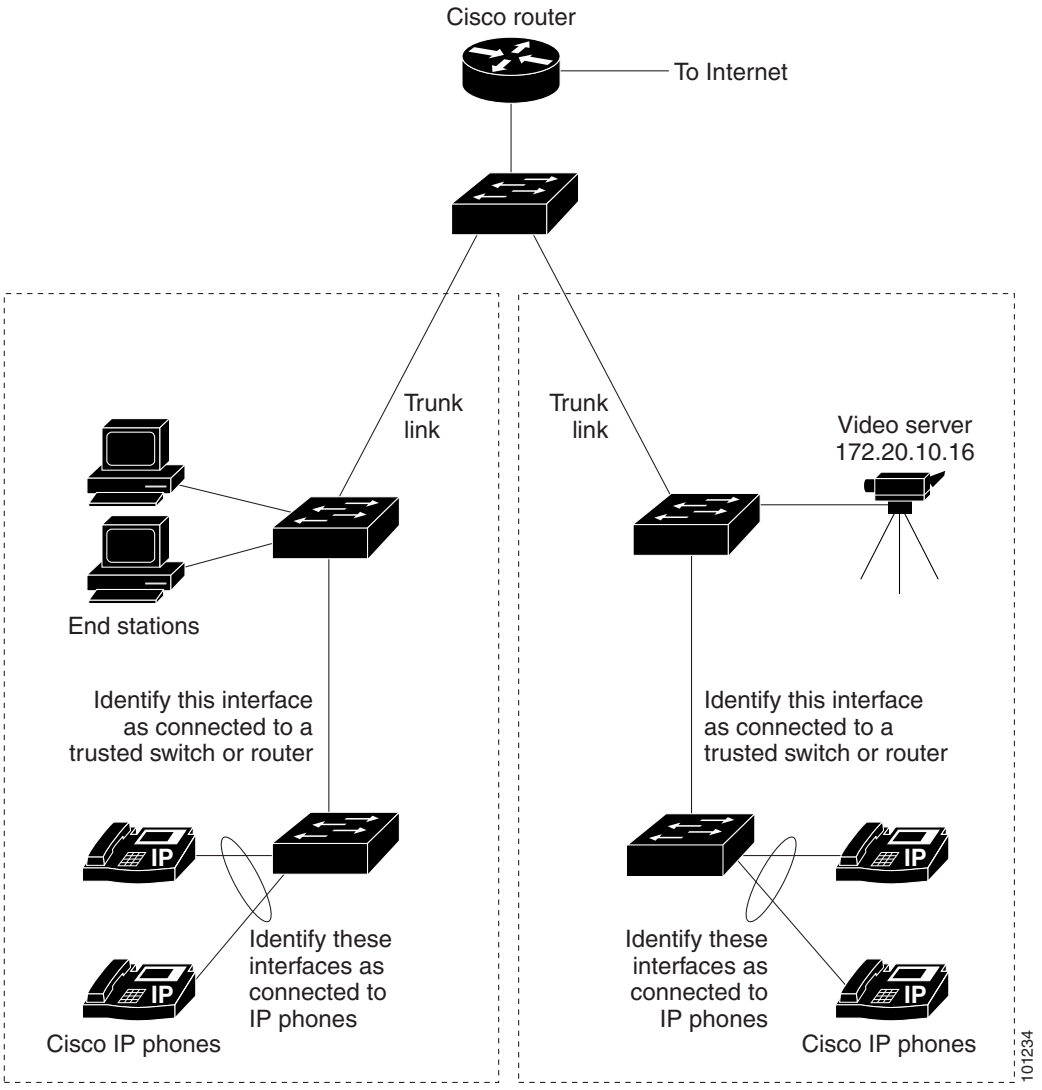
Configuration Examples for Auto-QoS

Auto-QoS Network: Example

This is an illustrated example that shows you how to implement auto-QoS in a network in which the VoIP traffic is prioritized over all other traffic. Auto-QoS is enabled on the switches in the wiring closets at the edge of the QoS domain.

For optimum QoS performance, enable auto-QoS on all the devices in the network.

Figure 36-1 Auto-QoS Configuration Example Network



Enabling Auto-QoS VOIP Trust: Example

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

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# auto qos voip trust
```

Additional References

The following sections provide references related to switch administration:

Related Documents

Related Topic	Document Title
Cisco IE 2000 commands	*Cisco IE 2000 Switch Command Reference*, Release 15.0(2)EC
Cisco IOS basic commands	*Cisco IOS Configuration Fundamentals Command Reference*
Standard QoS	*Chapter 35, "Configuring Standard QoS"*

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIBs	MIBs Link
—	To locate and download MIBs using Cisco IOS XR software, use the Cisco MIB Locator found at the following URL and choose a platform under the Cisco Access Products menu: http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport