Configuring Auto-QoS

Prerequisites for Auto-QoS

Before configuring standard QoS or auto-QoS, you must have a thorough understanding of these items:

- The types of applications used and the traffic patterns on your network.
- Traffic characteristics and needs of your network. Is the traffic bursty? Do you need to reserve bandwidth for voice and video streams?
- Bandwidth requirements and speed of the network.
- Location of congestion points in the network.

Auto-QoS VoIP Considerations

Before configuring auto-QoS for VoIP, you should be aware of this information:

- 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.

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

- When enabling auto-QoS with a Cisco IP Phone on a routed port, you must assign a static IP address to the IP phone.
- This release supports only Cisco IP SoftPhone Version 1.3(3) or later.
- Connected devices must use Cisco Call Manager Version 4 or later.
- 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.

Auto-QoS Enhanced Considerations

Auto-QoS is enhanced to support video. Automatic configurations are generated that classify and trust traffic from Cisco TelePresence systems and Cisco IP cameras.

Before configuring auto-QoS enhanced, you should be aware of this information:

- The **auto qos srnd4** global configuration command is generated as a result of enhanced auto-QoS configuration.

Restrictions for Auto-QoS

The following are restrictions for automatic QoS (auto-QoS):

- 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.
- 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.
- By default, the CDP is enabled on all ports. For auto-QoS to function properly, do not disable CDP.

Note You can enable auto-QoS on static, dynamic-access, voice VLAN access, and trunk ports.

Information About Configuring Auto-QoS

Auto-QoS Overview

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 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.

You can use auto-QoS commands to identify ports connected to the following Cisco devices:

- Cisco IP Phones
- Devices running the Cisco SoftPhone application
- Cisco TelePresence
- Cisco IP Camera
- Cisco digital media player

You also use the auto-QoS commands to identify ports that receive trusted traffic through an uplink. Auto-QoS then performs these functions:

- Detects the presence or absence of auto-QoS devices through conditional trusted interfaces.
- Configures QoS classification
- Configures egress queues

Auto-QoS Compact Overview

When you enter an auto-QoS command, the switch displays all the generated commands as if the commands were entered from the CLI. You can use the auto-QoS compact feature to hide the auto-QoS generated commands from the running configuration. This would make it easier to comprehend the running-configuration and also help to increase efficient usage of memory.

Generated Auto-QoS Configuration

By default, auto-QoS is disabled on all ports. Packets are not modified--the CoS, DSCP and IP precedence values in the packet are not changed.

When you enable the auto-QoS feature on the first port of the interface:

- Ingress packet label is used to categorize traffic, to assign packet labels, and to configure the ingress and egress queues.
- QoS is globally enabled (**mls qos** global configuration command), and other global configuration commands are automatically generated. (See Examples: Global Auto-QoS Configuration, on page 10).
- Switch enables the trusted boundary feature and uses the Cisco Discovery Protocol (CDP) to detect the presence of a supported device.
- Policing is used to determine whether a packet is in or out of profile and specifies the action on the packet.

VoIP Device Specifics

The following actions occur when you issue these auto-QoS commands on a port:

- **auto qos voip cisco-phone**—When you enter this command on a port at the network edge connected to a Cisco IP Phone, the switch enables the trusted boundary feature. 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 there is no

Cisco IP Phone, the ingress classification is set to not trust the QoS label in the packet. The policing is applied to the traffic matching the policy-map classification before the switch enables the trust boundary feature.

- **auto qos voip cisco-softphone** —When you enter this interface configuration command on a port at the network edge 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.
- **auto qos voip trust**—When you enter this 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).

The switch configures egress queues on the port according to the settings in the following tables.

Table 1: Traffic Types, Packet Labels, and Queues

	VoIP Data Traffic	VoIP Control Traffic	Routing Protocol Traffic	STP BPDU Traffic	Real-Time Video Traffic	All Other Traffic	
DSCP value	46	24, 26	48	56	34	–	
CoS value	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, 4)

The following table shows the generated auto-QoS configuration for the egress queues.

Table 2: 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	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

- 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 Examples: Global Auto-QoS Configuration, on page 10 to the port.

Effects of Auto-QoS on Running Configuration

When auto-QoS is enabled, the **auto qos** interface configuration commands and the generated global 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 may 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 are not applied, the previous running configuration is restored.

Effects of Auto-Qos Compact on Running Configuration

If auto-QoS compact is enabled:

- Only the auto-QoS commands entered from the CLI are displayed in running-config.
- The generated global and interface configurations are hidden.
- When you save the configuration, only the auto-qos commands you have entered are saved (and not the hidden configuration).
- When you reload the switch, the system detects and re-executes the saved auto-QoS commands and the AutoQoS SRND4.0 compliant config-set is generated .

Note Do not make changes to the auto-QoS-generated commands when auto-QoS compact is enabled, because user-modifications are overridden when the switch reloads.

When auto-qos global compact is enabled:

- **show derived-config** command can be used to view hidden AQC derived commands.
- AQC commands will not be stored to memory. They will be regenerated every time the switch is reloaded.
- When compaction is enabled, auto-qos generated commands should not be modified .
- If the interface is configured with auto-QoS and if AQC needs to be disabled, auto-qos should be disabled at interface level first.

How to Configure Auto-QoS

Configuring Auto-QoS

Enabling Auto-QoS

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

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**interface** *interface-id* **Example:** `Device(config)# interface gigabitethernet 3/0/1`	Specifies the port that is connected to a video device or the uplink port that is connected to another trusted switch or router in the network interior, and enters interface configuration mode.
Step 3	Use one of the following: • **auto qos voip** {**cisco-phone** | **cisco-softphone** | **trust**} • **auto qos video** {**cts** | **ip-camera** | **media-player**} • **auto qos classify** [**police**] • **auto qos trust** {**cos** | **dscp**} **Example:** `Device(config-if)# auto qos trust dscp`	Enables auto-QoS for VoIP. • **cisco-phone**—If 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**—The port is connected to device running the Cisco SoftPhone feature. • **trust**—The uplink port is connected to a trusted switch or router, and the VoIP traffic classification in the ingress packet is trusted. Enables auto-QoS for a video device. • **cts**—A port connected to a Cisco Telepresence system. • **ip-camera**—A port connected to a Cisco video surveillance camera. • **media-player**—A port connected to a CDP-capable Cisco digital media player. QoS labels of incoming packets are trusted only when the system is detected. Enables auto-QoS for classification. • **police**—Policing is set up by defining the QoS policy maps and applying them to ports (port-based QoS). Enables auto-QoS for trusted interfaces. • **cos**—Class of service.

	Command or Action	Purpose
		• **dscp**—Differentiated Services Code Point. • <cr>—Trust interface. **Note** To view a list of commands that are automatically generated by issuing one of the auto-QoS commands listed here, you need to be in debug mode. Refer to the *Catalyst 2960-XR Switch QoS Command Reference Guide* for examples of how to run the appropriate debug command to view a list of these commands.
Step 4	**exit** **Example:** `Device(config-if)# exit`	Returns to global configuration mode.
Step 5	**interface** *interface-id* **Example:** `Device(config)# interface gigabitethernet 2/0/1`	Specifies the switch port identified as connected to a trusted switch or router, and enters interface configuration mode.
Step 6	**auto qos trust** **Example:** `Device(config-if)# auto qos trust`	Enables auto-QoS on the port, and specifies that the port is connected to a trusted router or switch.
Step 7	**end** **Example:** `Device(config-if)# end`	Returns to privileged EXEC mode.
Step 8	**show auto qos interface** *interface-id* **Example:** `Device# show auto qos interface gigabitethernet 2/0/1`	Verifies your entries. This command displays the auto-QoS command on the interface on which auto-QoS was enabled. You can use the **show running-config** privileged EXEC command to display the auto-QoS configuration and the user modifications.

Enabling Auto-Qos Compact

To enable auto-Qos compact, enter this command:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**auto qos global compact** **Example:** `Device(config)# auto qos global compact`	Enables auto-Qos compact and generates (hidden) the global configurations for auto-QoS. You can then enter the auto-QoS command you want to configure in the interface configuration mode and the interface commands that the system generates are also hidden. To display the auto-QoS configuration that has been applied, use these the privileged EXEC commands: • **show derived-config** • **show policy-map** • **show access-list** • **show class-map** • **show table-map** • **show auto-qos** • **show policy-map interface** • **show ip access-lists** These commands will have keyword "**AutoQos-**".

What to do next

To disable auto-QoS compact, remove auto-Qos instances from all interfaces by entering the **no** form of the corresponding auto-QoS commands and then enter the **no auto qos global compact** global configuration command.

Troubleshooting Auto-QoS

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 you enable auto-QoS. For more information, see the **debug auto qos** command in the command reference for this release.

To disable auto-QoS on a port, use the **no** form of the **auto qos** command interface configuration command, such as **no auto qos voip**.

Note Auto-QoS generated global commands can also be removed manually if desired.

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).

Monitoring Auto-QoS

Table 3: Commands for Monitoring Auto-QoS

Command	Description
show auto qos [**interface** [*interface-type*]]	Displays the initial auto-QoS configurati You can compare the **show auto qos** and t to identify the user-defined QoS settings.
show mls qos [**aggregate policer** | **interface** | **maps** | **queue-set** | **stack-port** | **stack-qset** | **vlan**]	Displays information about the QoS config
show mls qos aggregate policer *policer_name*	Displays information about the QoS aggr affected by auto-QoS.
show mls qos interface [*interface-type* | **buffers** | **policers** | **queueing** | **statistics**]	Displays information about the QoS inter by auto-QoS.
show mls qos maps [**cos-dscp** | **cos-output-q** | **dscp-cos** | **dscp-mutation** | **dscp-output-q** | **ip-prec-dscp** | **policed-dscp**]	Displays information about the QoS map auto-QoS.
show mls qos queue-set *queue-set ID*	Displays information about the QoS queu by auto-QoS.
show mls qos stack-port buffers	Displays information about the QoS stacl affected by auto-QoS.
show mls qos stack-qset	Displays information about the QoS stacl affected by auto-QoS.
show running-config	Displays information about the QoS config You can compare the **show auto qos** and t to identify the user-defined QoS settings.

Configuration Examples for Auto-Qos

Examples: Global Auto-QoS Configuration

The following table describes the automatically generated commands for auto-QoS and enhanced auto-QoS by the switch.

Table 4: Generated Auto-QoS Configuration

Description	Automatically Generated Command {voip}	Enhanced Au
The switch automatically enables standard QoS and configures the CoS-to-DSCP map (maps CoS values in incoming packets to a DSCP value).	Device(config)# **mls qos** Device(config)# **mls qos map cos-dscp** **0 8 16 26 32 46 48 56**	Device(conf Device(conf **0 8 16 24 3**
The switch automatically maps CoS values to an egress queue and to a threshold ID.	Device(config)# **no mls qos srr-queue output cos-map** Device(config)# **mls qos srr-queue output cos-map queue 1 threshold 3 5** Device(config)# **mls qos srr-queue output cos-map queue 2 threshold 3 3 6 7** Device(config)# **mls qos srr-queue output cos-map queue 3 threshold 3 2 4** Device(config)# **mls qos srr-queue output cos-map queue 4 threshold 2 1** Device(config)# **mls qos srr-queue output cos-map queue 4 threshold 3 0**	Device(conf **output cos-** Device(conf **output cos-** Device(conf **output cos-** Device(conf **output cos-** Device(conf **output cos-** Device(conf **output cos-** Device(conf **output cos-**

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

Description	Automatically Generated Command {voip}	Enhanced Au
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.	Device(config)# **mls qos queue-set output 1 threshold 1 138 138 92 138** Device(config)# **mls qos queue-set output 1 threshold 2 138 138 92 400** Device(config)# **mls qos queue-set output 1 threshold 3 36 77 100 318** Device(config)# **mls qos queue-set output 1 threshold 4 20 50 67 400** Device(config)# **mls qos queue-set output 2 threshold 1 149 149 100 149** Device(config)# **mls qos queue-set output 2 threshold 2 118 118 100 235** Device(config)# **mls qos queue-set output 2 threshold 3 41 68 100 272** Device(config)# **mls qos queue-set output 2 threshold 4 42 72 100 242** Device(config)# **mls qos queue-set output 1 buffers 10 10 26 54** Device(config)# **mls qos queue-set output 2 buffers 16 6 17 61** Device(config-if)# **priority-queue out** Device(config-if)# **srr-queue bandwidth share 10 10 60 20**	Device(conf **output 1 th** Device(conf **output 1 th** Device(conf **output 1 th** Device(conf **output 1 th** Device(conf **output 1 bu**

Examples: Auto-QoS Generated Configuration for VoIP Devices

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.

```
Device(config-if)# mls qos trust device cisco-phone
```

If you entered the **auto qos voip cisco-softphone** command, the switch automatically creates class maps and policy maps.

```
Device(config)# mls qos map policed-dscp 24 26 46 to 0
Device(config)# class-map match-all AutoQoS-VoIP-RTP-Trust
Device(config-cmap)# match ip dscp ef
Device(config)# class-map match-all AutoQoS-VoIP-Control-Trust
Device(config-cmap)# match ip dscp cs3 af31
Device(config)# policy-map AutoQoS-Police-SoftPhone
Device(config-pmap)# class AutoQoS-VoIP-RTP-Trust
Device(config-pmap-c)# set dscp ef
Device(config-pmap-c)# police 320000 8000 exceed-action policed-dscp-transmit
Device(config-pmap)# class AutoQoS-VoIP-Control-Trust
Device(config-pmap-c)# set dscp cs3
Device(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.

```
Device(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.

```
Device(config-if)# mls qos trust device cisco-phone
```

If you entered the **auto qos voip cisco-softphone** command, the switch automatically creates class maps and policy maps.

```
Device(config)# mls qos map policed-dscp 24 26 46 to 0
Device(config)# class-map match-all AutoQoS-VoIP-RTP-Trust
Device(config-cmap)# match ip dscp ef
Device(config)# class-map match-all AutoQoS-VoIP-Control-Trust
Device(config-cmap)# match ip dscp cs3 af31
Device(config)# policy-map AutoQoS-Police-CiscoPhone
Device(config-pmap)# class AutoQoS-VoIP-RTP-Trust
Device(config-pmap-c)# set dscp ef
Device(config-pmap-c)# police 320000 8000 exceed-action policed-dscp-transmit
Device(config-pmap)# class AutoQoS-VoIP-Control-Trust
Device(config-pmap-c)# set dscp cs3
Device(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.

```
Device(config-if)# service-policy input AutoQoS-Police-SoftPhone
```

Examples: Auto-QoS Generated Configuration For Enhanced Video, Trust, and Classify Devices

If you entered the following enhanced auto-QoS commands, the switch configures a CoS-to-DSCP map (maps CoS values in incoming packets to a DSCP value):

- **auto qos video cts**
- **auto qos video ip-camera**
- **auto qos video media-player**
- **auto qos trust**
- **auto qos trust cos**
- **auto qos trust dscp**

  The following command is initiated after entering one of the above auto-QoS commands:

  ```
  Device(config)# mls qos map cos-dscp 0 8 16 24 32 46 48 56
  ```

Note No class maps and policy maps are configured.

If you entered the **auto qos classify** command, the switch automatically creates class maps and policy maps (as shown below).

```
Device(config)# mls qos map policed-dscp 0 10 18 24 26 46 to 8
Device(config)# mls qos map cos-dscp 0 8 16 24 32 46 48 56
Device(config)# class-map match-all AUTOQOS_MULTIENHANCED_CONF_CLASS
Device(config-cmap)# match access-group name AUTOQOS-ACL-MULTIENHANCED-CONF
Device(config)# class-map match-all AUTOQOS_DEFAULT_CLASS
Device(config-cmap)# match access-group name AUTOQOS-ACL-DEFAULT
Device(config)# class-map match-all AUTOQOS_TRANSACTION_CLASS
Device(config-cmap)# match access-group name AUTOQOS-ACL-TRANSACTIONAL-DATA
Device(config)# class-map match-all AUTOQOS_SIGNALING_CLASS
Device(config-cmap)# match access-group name AUTOQOS-ACL-SIGNALING
Device(config)# class-map match-all AUTOQOS_BULK_DATA_CLASS
Device(config-cmap)# match access-group name AUTOQOS-ACL-BULK-DATA
Device(config)# class-map match-all AUTOQOS_SCAVANGER_CLASS
Device(config-cmap)# match access-group name AUTOQOS-ACL-SCAVANGER
Device(config)# policy-map AUTOQOS-SRND4-CLASSIFY-POLICY
Device(config-pmap)# class AUTOQOS_MULTIENHANCED_CONF_CLASS
Device(config-pmap-c)# set dscp af41
Device(config-pmap)# class AUTOQOS_BULK_DATA_CLASS
Device(config-pmap-c)# set dscp af11
Device(config-pmap)# class AUTOQOS_TRANSACTION_CLASS
Device(config-pmap-c)# set dscp af21
Device(config-pmap)# class AUTOQOS_SCAVANGER_CLASS
Device(config-pmap-c)# set dscp cs1
Device(config-pmap)# class AUTOQOS_SIGNALING_CLASS
Device(config-pmap-c)# set dscp cs3
Device(config-pmap)# class AUTOQOS_DEFAULT_CLASS
Device(config-pmap-c)# set dscp default
;
Device(config-if)# service-policy input AUTOQOS-SRND4-CLASSIFY-POLICY
```

If you entered the **auto qos classify police** command, the switch automatically creates class maps and policy maps (as shown below).

```
Device(config)# mls qos map policed-dscp 0 10 18 24 26 46 to 8
Device(config)# mls qos map cos-dscp 0 8 16 24 32 46 48 56
Device(config)# class-map match-all AUTOQOS_MULTIENHANCED_CONF_CLASS
Device(config-cmap)# match access-group name AUTOQOS-ACL-MULTIENHANCED-CONF
Device(config)# class-map match-all AUTOQOS_DEFAULT_CLASS
Device(config-cmap)# match access-group name AUTOQOS-ACL-DEFAULT
Device(config)# class-map match-all AUTOQOS_TRANSACTION_CLASS
Device(config-cmap)# match access-group name AUTOQOS-ACL-TRANSACTIONAL-DATA
Device(config)# class-map match-all AUTOQOS_SIGNALING_CLASS
Device(config-cmap)# match access-group name AUTOQOS-ACL-SIGNALING
Device(config)# class-map match-all AUTOQOS_BULK_DATA_CLASS
Device(config-cmap)# match access-group name AUTOQOS-ACL-BULK-DATA
Device(config)# class-map match-all AUTOQOS_SCAVANGER_CLASS
Device(config-cmap)# match access-group name AUTOQOS-ACL-SCAVANGER
Device(config)# policy-map AUTOQOS-SRND4-CLASSIFY-POLICE-POLICY
Device(config-pmap)# class AUTOQOS_MULTIENHANCED_CONF_CLASS
Device(config-pmap-c)# set dscp af41
Device(config-pmap-c)# police 5000000 8000 exceed-action drop
```

```
Device(config-pmap)# class AUTOQOS_BULK_DATA_CLASS
Device(config-pmap-c)# set dscp af11
Device(config-pmap-c)# police 10000000 8000 exceed-action policed-dscp-transmit
Device(config-pmap)# class AUTOQOS_TRANSACTION_CLASS
Device(config-pmap-c)# set dscp af21
Device(config-pmap-c)# police 10000000 8000 exceed-action policed-dscp-transmit
Device(config-pmap)# class AUTOQOS_SCAVANGER_CLASS
Device(config-pmap-c)# set dscp cs1
Device(config-pmap-c)# police 10000000 8000 exceed-action drop
Device(config-pmap)# class AUTOQOS_SIGNALING_CLASS
Device(config-pmap-c)# set dscp cs3
Device(config-pmap-c)# police 32000 8000 exceed-action drop
Device(config-pmap)# class AUTOQOS_DEFAULT_CLASS
Device(config-pmap-c)# set dscp default
Device(config-pmap-c)# police 10000000 8000 exceed-action policed-dscp-transmit
;
Device(config-if)# service-policy input AUTOQOS-SRND4-CLASSIFY-POLICE-POLICY
```

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

```
Device(config)# mls qos map policed-dscp 0 10 18 24 26 46 to 8
Device(config)# mls qos map cos-dscp 0 8 16 24 32 46 48 56
Device(config)# class-map match-all AUTOQOS_VOIP_DATA_CLASS
Device(config-cmap)# match ip dscp ef
Device(config)# class-map match-all AUTOQOS_DEFAULT_CLASS
Device(config-cmap)# match access-group name AUTOQOS-ACL-DEFAULT
Device(config)# class-map match-all AUTOQOS_VOIP_SIGNAL_CLASS
Device(config-cmap)# match ip dscp cs3
Device(config)# policy-map AUTOQOS-SRND4-CISCOPHONE-POLICY
Device(config-pmap)# class AUTOQOS_VOIP_DATA_CLASS
Device(config-pmap-c)# set dscp ef
Device(config-pmap-c)# police 128000 8000 exceed-action policed-dscp-transmit
Device(config-pmap)# class AUTOQOS_VOIP_SIGNAL_CLASS
Device(config-pmap-c)# set dscp cs3
Device(config-pmap-c)# police 32000 8000 exceed-action policed-dscp-transmit
Device(config-pmap)# class AUTOQOS_DEFAULT_CLASS
Device(config-pmap-c)# set dscp default
Device(config-pmap-c)# police 10000000 8000 exceed-action policed-dscp-transmit
;
Device(config-if)# service-policy input AUTOQOS-SRND4-CISCOPHONE-POLICY
```

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

```
Device(config)# mls qos map policed-dscp 0 10 18 24 26 46 to 8
Device(config)# mls qos map cos-dscp 0 8 16 24 32 46 48 56
Device(config)# class-map match-all AUTOQOS_MULTIENHANCED_CONF_CLASS
Device(config-cmap)# match access-group name AUTOQOS-ACL-MULTIENHANCED-CONF
Device(config)# class-map match-all AUTOQOS_VOIP_DATA_CLASS
Device(config-cmap)# match ip dscp ef
Device(config)# class-map match-all AUTOQOS_DEFAULT_CLASS
Device(config-cmap)# match access-group name AUTOQOS-ACL-DEFAULT
Device(config)# class-map match-all AUTOQOS_TRANSACTION_CLASS
Device(config-cmap)# match access-group name AUTOQOS-ACL-TRANSACTIONAL-DATA
Device(config)# class-map match-all AUTOQOS_VOIP_SIGNAL_CLASS
Device(config-cmap)# match ip dscp cs3
Device(config)# class-map match-all AUTOQOS_SIGNALING_CLASS
Device(config-cmap)# match access-group name AUTOQOS-ACL-SIGNALING
Device(config)# class-map match-all AUTOQOS_BULK_DATA_CLASS
Device(config-cmap)# match access-group name AUTOQOS-ACL-BULK-DATA
Device(config)# class-map match-all AUTOQOS_SCAVANGER_CLASS
```

```
Device(config-cmap)# match access-group name AUTOQOS-ACL-SCAVANGER

Device(config)# policy-map AUTOQOS-SRND4-SOFTPHONE-POLICY
Device(config-pmap)# class AUTOQOS_VOIP_DATA_CLASS
Device(config-pmap-c)# set dscp ef
Device(config-pmap-c)# police 128000 8000 exceed-action policed-dscp-transmit
Device(config-pmap)# class AUTOQOS_VOIP_SIGNAL_CLASS
Device(config-pmap-c)# set dscp cs3
Device(config-pmap-c)# police 32000 8000 exceed-action policed-dscp-transmit
Device(config-pmap)#class AUTOQOS_MULTIENHANCED_CONF_CLASS
Device(config-pmap-c)#set dscp af41
Device(config-pmap-c)# police 5000000 8000 exceed-action drop
Device(config-pmap)# class AUTOQOS_BULK_DATA_CLASS
Device(config-pmap-c)# set dscp af11
Device(config-pmap-c)# police 10000000 8000 exceed-action policed-dscp-transmit
Device(config-pmap)# class AUTOQOS_TRANSACTION_CLASS
Device(config-pmap-c)# set dscp af21
Device(config-pmap-c)# police 10000000 8000 exceed-action policed-dscp-transmit
Device(config-pmap)# class AUTOQOS_SCAVANGER_CLASS
Device(config-pmap-c)# set dscp cs1
Device(config-pmap-c)# police 10000000 8000 exceed-action drop
Device(config-pmap)# class AUTOQOS_SIGNALING_CLASS
Device(config-pmap-c)# set dscp cs3
Device(config-pmap-c)# police 32000 8000 exceed-action drop
Device(config-pmap)# class AUTOQOS_DEFAULT_CLASS
Device(config-pmap-c)# set dscp default
;
Device(config-if)# service-policy input AUTOQOS-SRND4-SOFTPHONE-POLICY
```

auto qos global compact

The following is an example of the **auto qos global compact** command.

```
Device# configure terminal
Device(config)# auto qos global compact
Device(config)# interface GigabitEthernet1/2
Device(config-if)# auto qos voip cisco-phone

Device# show auto-qos

GigabitEthernet1/2
auto qos voip cisco-phone

Device# show running-config interface GigabitEthernet 1/0/2

interface GigabitEthernet1/0/2
auto qos voip cisco-phone
end
```

Where to Go Next for Auto-QoS

Review the QoS documentation if you require any specific QoS changes to your auto-QoS configuration.

Additional References

Related Documents

Related Topic	Document Title
For complete syntax and usage information for the commands used in this book.	*Catalyst 2960-XR Switch Quality of Service Command Reference*

Standards and RFCs

Standard/RFC	Title
—	—

MIBs

MIB	MIBs Link
All the supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature History and Information for Auto-QoS

Release	Modification
Cisco IOS Release 15.0(2)EX1	This feature was introduced.