Configuring AutoQoS

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.

Restrictions for Auto-QoS

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

- Ternary content-addressable memory (TCAM) sharing of policy-map (policer/marking) across ports is not supported. Because of this, the number of interfaces on which auto-QoS/QoS policy-map can be applied is limited.
- The same TCAM region must be used for both security Access control lists (ACLs) and ACLs used via policy map.
- Policy-maps with the **match ip dscp** command matches both IPv4 and IPv6 addresses, which limits the scale number to 16 class-maps. One TCAM entry is created for IPv4 and one TCAM entry for IPv6.

- Per ASIC, 8 TCP port comparators and 8 UDP port comparators are supported, and each gt (greater than)/lt (less than)/neq (not equal) operator uses 1 port comparator, and each range operator uses 2 port comparators. A policy-map with this combination affects the TCAM scale and number of interfaces to which the policy-map can be attached.
- The following restrictions apply to IPv4 ACL network interfaces:
  - When controlling access to an interface, you can use a named or numbered ACL.
  - If you apply an ACL to a Layer 3 interface, and routing is not enabled on the switch, the ACL only filters packets that are intended for the CPU, such as SNMP, Telnet, or web traffic.
  - You do not have to enable routing to apply ACLs on Layer 2 interfaces.
- Deny ACLs are not supported on QoS policy-maps.

Information about Configuring Auto-QoS

This section provides 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

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 9).
- Switch enables the trusted boundary feature and uses the Cisco Discovery Protocol 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 activities occur when you issue these auto-QoS commands on a port:

- When you enter the **auto qos voip cisco-phone** 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.
- When you enter the **auto qos voip cisco-softphone** 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.
- When you enter the **auto qos voip trust** interface configuration command on a port connected to the network interior, the switch trusts the CoS value for nonrouted ports or the DSCP value for routed ports in ingress packets (the assumption is that traffic has already been classified by other edge devices).

Table 1: Traffic Types, Packet Labels, and Queues

<table>
<tr><th></th><th>VoIP Data Traffic</th><th>VoIP Control Traffic</th><th>Routing Protocol Traffic</th><th>STP BPDU Traffic</th><th>Real-Time Video Traffic</th><th colspan="2">All Other Traffic</th></tr>
<tr><td>DSCP value</td><td>46</td><td>24, 26</td><td>48</td><td>56</td><td>34</td><td colspan="2">–</td></tr>
<tr><td>CoS value</td><td>5</td><td>3</td><td>6</td><td>7</td><td>3</td><td colspan="2">–</td></tr>
<tr><td>CoS-to-Egress queue map</td><td>4, 5 (queue 1)</td><td colspan="3">2, 3, 6, 7 (queue 2)</td><td>0 (queue 2)</td><td>2 (queue 3)</td><td>0, 1 (queue 4)</td></tr>
</table>

- 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 9 to the port.

Enhanced Auto-QoS for Video, Trust, and Classification

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

Auto-QoS Configuration Migration

Auto-QoS configuration migration from legacy auto-QoS to enhanced auto-QoS occurs when:

- A switch is booted with a 12.2(55)SE image and QoS is not enabled.

  Any video or voice trust configuration on the interface automatically generates enhanced auto-QoS commands.

- A switch is enabled with QoS, these guidelines take effect:
  - If you configure the interface for conditional trust on a voice device, only the legacy auto-QoS VoIP configuration is generated.
  - If you configure the interface for conditional trust on a video device, the enhanced auto-QoS configuration is generated.
  - If you configure the interface with classification or conditional trust based on the new interface auto-QoS commands, enhanced auto-QoS configuration is generated.

- Auto-QoS migration happens after a new device is connected when the **auto qos srnd4** global configuration command is enabled.

Note If an interface previously configured with legacy auto-QoS migrates to enhanced auto-QoS, voice commands and configuration are updated to match the new global QoS commands.

Auto-QoS configuration migration from enhanced auto-QoS to legacy auto-QoS can occur only when you disable all existing auto-QoS configurations from the interface.

Auto-QoS Configuration Guidelines

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

- After auto-QoS is enabled, do not modify a policy map that includes *AutoQoS* in its name. If you need to modify the policy map, make a copy of it, and change the copied policy map. 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.
- You can enable auto-QoS on static, dynamic-access, voice VLAN access, and trunk ports.

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

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 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.

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.

How to Configure Auto-QoS

This section provides information about how to configure 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 1/0/1`
	`Or`
	`Device(config)# interface fastethernet 1/0/1`
		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.

	Command or Action	Purpose
		• **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. • **dscp**: Differentiated Services Code Point. • <cr>—Trust interface.
Step 4	**exit** **Example:** `Device(config-if)# exit`	Returns to global configuration mode.

Step 5	**interface** *interface-id*
	Example:
	`Device(config)# interface gigabitethernet 1/0/1`
	`Or`
	`Device(config)# interface fastethernet 1/0/1`
		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(config)# show auto qos interface gigabitethernet 1/0/1`
	`Or`
	`Device(config)# show auto qos interface fastethernet 1/0/1`
		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.

Troubleshooting Auto-QoS

To troubleshoot auto-QoS, use the **debug auto qos** privileged EXEC command. 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**. 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).

Monitoring Auto-QoS

Table 2: Commands for Monitoring Auto-QoS

Command	Description
show auto qos [**interface** [*interface-type*]]	Displays the initial auto-QoS configuration. You can compare the **show auto qos** and the **show running-config** command output to identify the user-defined QoS settings.
show mls qos [**interface** | **maps**]	Displays information about the QoS configuration that might be affected by auto-QoS.
show mls qos interface [*interface-type* | **queueing** | **statistics**]	Displays information about the QoS interface configuration that might be affected by auto-QoS.
show mls qos maps [**cos-output-q** | **dscp-mutation** | **dscp-output-q**]	Displays information about the QoS maps configuration that might be affected by auto-QoS.
show running-config	Displays information about the QoS configuration that might be affected by auto-QoS. You can compare the **show auto qos** and the **show running-config** command output to identify the user-defined QoS settings.

Configuration Example for Auto-QoS

The following sections provide 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 3: Generated Auto-QoS Configuration

Description	Automatically Generated Command {voip}
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 1 4** Device(config)# **mls qos srr-queue output cos-map queue 2 threshold 1 2 6 7 6 7** Device(config)# **mls qos srr-queue output cos-map queue 2 threshold 2 3 4** Device(config)# **mls qos srr-queue output cos-map queue 3 threshold 2 0** Device(config)# **mls qos srr-queue output cos-map queue 4 threshold 2 1**
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 2 32 33 40 41 42 43 44 45** Device(config)# **mls qos srr-queue output dscp-map queue 1 threshold 2 46 47** Device(config)# **mls qos srr-queue output dscp-map queue 2 threshold 1 16 17 18 19 20 21 22 23** Device(config)# **mls qos srr-queue output dscp-map queue 2 threshold 1 26 27 28 29 30 31 34 35** Device(config)# **mls qos srr-queue output dscp-map queue 2 threshold 1 36 37 38 39** Device(config)# **mls qos srr-queue output dscp-map queue 2 threshold 2 24 48 49 50 51 52 53 54** Device(config)# **mls qos srr-queue output dscp-map queue 2 threshold 2 55 56 57 58 59 60 61 62** Device(config)# **mls qos srr-queue output dscp-map queue 2 threshold 2 63** Device(config)# **mls qos srr-queue output dscp-map queue 3 threshold 1 0 1 2 3 4 5 6 7** Device(config)# **mls qos srr-queue output dscp-map queue 4 threshold 1 8 9 10 11 12 13 14 15**

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**

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

```
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)# 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)# police 5000000 8000 exceed-action drop
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)# police 10000000 8000 exceed-action drop
Device(config-pmap)# class AUTOQOS_SIGNALING_CLASS
Device(config-pmap-c)# set dscp cs3
Device(config-pmap)# police 32000 8000 exceed-action drop
Device(config-pmap)# class AUTOQOS_DEFAULT_CLASS
Device(config-pmap-c)# set dscp default
```

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

```
Device(config)# class-map match-all AUTOQOS_VOIP_DATA_CLASS
Device(config-cmap)# match ip dscp ef
Device(config)# class-map match-all AUTOQOS_VOIP_VIDEO_CLASS
Device(config-cmap)# match ip dscp af41
Device(config)# class-map match-all AUTOQOS_VOIP_SIGNAL_CLASS
Device(config-cmap)# match ip dscp cs3
Device(config)# class-map match-all AUTOQOS_DEFAULT_CLASS
Device(config-cmap)# match access-group name AUTOQOS-ACL-DEFAULT
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)# class AUTOQOS_VOIP_VIDEO_CLASS
Device(config-pmap-c)# set dscp af41
Device(config-pmap)# class AUTOQOS_VOIP_SIGNAL_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-CISCOPHONE-POLICY
```

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

```
Device(config)# class-map match-all AUTOQOS_VOIP_DATA_CLASS
Device(config-cmap)# match ip dscp ef
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_BULK_DATA_CLASS
Device(config-cmap)# match access-group name AUTOQOS-ACL-BULK-DATA
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_SCAVANGER_CLASS
Device(config-cmap)# match access-group name AUTOQOS-ACL-SCAVANGER
Device(config)# class-map match-all AUTOQOS_SIGNALING_CLASS
Device(config-cmap)# match access-group name AUTOQOS-ACL-SIGNALING

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)# class AUTOQOS_MULTIENHANCED_CONF_CLASS
Device(config-pmap-c)# set dscp af41
Device(config-pmap)#police 5000000 8000 exceed-action drop
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)# police 10000000 8000 exceed-action drop
Device(config-pmap)# class AUTOQOS_SIGNALING_CLASS
Device(config-pmap-c)# set dscp cs3
Device(config-pmap)# 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
```

Additional References for Auto-QoS

Related Documents

Related Topic	Document Title
For complete syntax and usage information for the commands used in this chapter.	*Cisco IOS Quality of Service Solutions Command Reference*

Feature History and Information for Auto-QoS

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 4: Feature Information for Configuring Auto-QoS

Feature Name	Releases	Feature Information
Auto-QoS	Cisco IOS Release 15.2(7)E1	This feature was introduced.