Configuring Auto-QoS

Prerequisites for Auto-QoS

The prerequisites for auto-QoS are the same as the prerequisites for standard QoS.

Restrictions for Auto-QoS

The following are restrictions for auto-QoS:

- Auto-qos is not supported on SVI interfaces.
- Do not configure the `auto qos voip cisco-phone` option for IP phones that support video. This option causes DSCP markings of video packets to get overwritten, because these packets do not have Expedited Forwarding priority, which results in these packets getting classified in the class-default class.

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.

The switch employs the MQC model. This means that instead of using certain global configurations, auto-QoS applied to any interface on a switch configures several global class maps and policy maps.
Auto-QoS matches traffic and assigns each matched packet to qos-groups. This allows the output policy map to put specific qos-groups into specific queues, including into the priority queue.

QoS is needed in both directions, both on inbound and outbound. When inbound, the switch port needs to trust the DSCP in the packet (done by default). When outbound, the switch port needs to give voice packets "front of line" priority. If voice is delayed too long by waiting behind other packets in the outbound queue, the end host drops the packet because it arrives outside of the receive window for that packet.

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.

Auto-QoS Global Configuration Templates

In general, an auto-QoS command generates a series of class maps that either match on ACLs or on DSCP and/or CoS values to differentiate traffic into application classes. An input policy is also generated, which matches the generated classes and in some cases, polices the classes to a set bandwidth. Eight egress-queue class maps are generated. The actual egress output policy assigns a queue to each one of these eight egress-queue class maps.

The auto-QoS commands only generate templates as needed. For example, the first time any new auto-QoS command is used, global configurations that define the eight queue egress-service-policy are generated. From this point on, auto-QoS commands applied to other interfaces do not generate templates for egress queuing because all auto-QoS commands rely on the same eight queue models, which have already been generated from the first time a new auto-QoS command was used.

Auto-QoS Policy and Class Maps

After entering the appropriate auto-QoS command, the following actions occur:

- Specific class maps are created.
- Specific policy maps (input and output) are created.
- Policy maps are attached to the specified interface.
- Trust level for the interface is configured.

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**

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

**SUMMARY STEPS**

1. `configure terminal`
2. `interface interface-id`
3. Depending on your auto-QoS configuration, use one of the following commands:
   - `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}
4. `end`
5. show auto qos interface interface-id

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td>Example: device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2 interface interface-id</td>
<td>Specifies the port that is connected to a VoIP port, video device, or the uplink port that is connected to another trusted interface.</td>
</tr>
<tr>
<td>Example: device(config)# interface gigabitethernet 3/0/1</td>
<td></td>
</tr>
<tr>
<td>Step 3 Depending on your auto-QoS configuration, use one of the following commands:</td>
<td>The following commands enable auto-QoS for VoIP:</td>
</tr>
<tr>
<td>• auto qos voip {cisco-phone</td>
<td>cisco-softphone</td>
</tr>
<tr>
<td>• auto qos video {cts</td>
<td>ip-camera</td>
</tr>
<tr>
<td>• auto qos classify [police]</td>
<td>• auto qos voip cisco-softphone—The port is connected to device running the Cisco SoftPhone feature. This command generates a QoS configuration for interfaces connected to PCs running the Cisco IP SoftPhone application and mark, as well as police traffic coming from such interfaces. Ports configured with this command are considered untrusted.</td>
</tr>
<tr>
<td>• auto qos trust {cos</td>
<td>dscp}</td>
</tr>
<tr>
<td>Example: device(config-if)# auto qos trust dscp</td>
<td>The following commands enable auto-QoS for the specified video device (system, camera, or media player):</td>
</tr>
<tr>
<td></td>
<td>• auto qos video cts—A port connected to a Cisco Telepresence system. QoS labels of incoming packets</td>
</tr>
</tbody>
</table>
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>• auto qos video ip-camera</td>
<td>A port connected to a Cisco video surveillance camera. QoS labels of incoming packets are only trusted (conditional trust through CDP) when a Cisco camera is detected.</td>
</tr>
<tr>
<td>• auto qos video media-player</td>
<td>A port connected to a CDP-capable Cisco digital media player. QoS labels of incoming packets are only trusted (conditional trust through CDP) when a digital media player is detected.</td>
</tr>
</tbody>
</table>

The following command enables auto-QoS for classification:

• auto qos classify police — This command generates a QoS configuration for untrusted interfaces. The configuration places a service-policy on the interface to classify traffic coming from untrusted desktops/devices and mark them accordingly. The service-policies generated do police.

The following commands enable auto-QoS for trusted interfaces:

• auto qos trust cos — Class of service.

• auto qos trust dscp — Differentiated Services Code Point.

### Step 4

End

Example:

device(config-if)# end

Returns to privileged EXEC mode.

### Step 5

Show auto qos interface interface-id

Example:

device# show auto qos interface gigabitethernet 3/0/1

(Optional) Displays the auto-QoS command on the interface on which auto-QoS was enabled. Use the show running-config command to display the auto-QoS configuration and user modifications.

## Upgrading Auto-QoS

### Before you begin

Prior to upgrading, you need to remove all auto-QoS configurations currently on the switch. This sample procedure describes that process.
After following this sample procedure, you must then reboot the switch with the new or upgraded software image and reconfigure auto-QoS.

**SUMMARY STEPS**

1. `show auto qos`
2. `no auto qos`
3. `show running-config | i autoQos`
4. `no policy-map policy-map_name`
5. `show running-config | i AutoQoS`
6. `show auto qos`
7. `write memory`

**DETAILED STEPS**

**Step 1** `show auto qos`

**Example:**

```
device# show auto qos
GigabitEthernet2/0/3
  auto qos voip cisco-phone
GigabitEthernet2/0/27
  auto qos voip cisco-softphone
```

In privileged EXEC mode, record all current auto QoS configurations by entering this command.

**Step 2** `no auto qos`

**Example:**

```
device(config-if)# no auto qos
```

In interface configuration mode, run the appropriate `no auto qos` command on each interface that has an auto QoS configuration.

**Step 3** `show running-config | i autoQos`

**Example:**

```
device# show running-config | i autoQos
```

Return to privileged EXEC mode, and record any remaining auto QoS maps class maps, policy maps, access lists, table maps, or other configurations by entering this command.

**Step 4** `no policy-map policy-map_name`

**Example:**

```
device)config# no policy-map pmap_101
device)config# no class-map cmap_101
```
device)config# no ip access-list extended AutoQos-101
device)config# no table-map 101
device)config# no table-map policed-dscp

In global configuration mode, remove the QoS class maps, policy maps, access-lists, table maps, and any other auto QoS configurations by entering these commands:

- no policy-map policy-map-name
- no class-map class-map-name
- no ip access-list extended Auto-QoS-x
- no table-map table-map-name
- no table-map policed-dscp

**Step 5** show running-config | i AutoQoS

Example:

device# show running-config | i AutoQoS

Return to privileged EXEC mode, run this command again to ensure that no auto-QoS configuration or remaining parts of the auto-QoS configuration exists.

**Step 6** show auto qos

Example:

device# show auto qos

Run this command to ensure that no auto-QoS configuration or remaining parts of the configuration exists.

**Step 7** write memory

Example:

device# write memory

Write the changes to the auto QoS configuration to NV memory by entering the **write memory** command.

---

**What to do next**

Reboot the switch with the new or upgraded software image.

After rebooting with the new or upgraded software image, re-configure auto-QoS for the appropriate switch interfaces as determined by running the **show auto qos** command described in step 1.

---

**Note**

There is only one table-map for exceed and another table-map for violate markdown per switch. If the switch already has a table-map under the exceed action, then the auto-qos policy cannot be applied.
Enabling Auto-Qos Compact

To enable auto-Qos compact, enter this command:

SUMMARY STEPS

1. configure terminal
2. auto qos global compact

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td>Example: device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2 auto qos global compact</td>
<td>Enables auto-Qos compact and generates (hidden) the global configurations for auto-QoS.</td>
</tr>
<tr>
<td>Example: device(config)# auto qos global compact</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>To display the auto-QoS configuration that has been applied, use these the privileged EXEC commands:</td>
</tr>
<tr>
<td></td>
<td>• show derived-config</td>
</tr>
<tr>
<td></td>
<td>• show policy-map</td>
</tr>
<tr>
<td></td>
<td>• show access-list</td>
</tr>
<tr>
<td></td>
<td>• show class-map</td>
</tr>
<tr>
<td></td>
<td>• show table-map</td>
</tr>
<tr>
<td></td>
<td>• show auto-qos</td>
</tr>
<tr>
<td></td>
<td>• show policy-map interface</td>
</tr>
<tr>
<td></td>
<td>• show ip access-lists</td>
</tr>
<tr>
<td></td>
<td>These commands will have keyword &quot;AutoQos-&quot;.</td>
</tr>
</tbody>
</table>

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.
Monitoring Auto-QoS

Table 1: Commands for Monitoring Auto-QoS

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show auto qos [interface [interface-id]]</code></td>
<td>Displays the initial auto-QoS configuration. You can compare the <code>show auto qos</code> and the <code>show running-config</code> command output to identify the user-defined QoS settings.</td>
</tr>
<tr>
<td><code>show running-config</code></td>
<td>Displays information about the QoS configuration that might be affected by auto-QoS. You can compare the <code>show auto qos</code> and the <code>show running-config</code> command output to identify the user-defined QoS settings.</td>
</tr>
<tr>
<td><code>show derived-config</code></td>
<td>Displays the hidden <code>mls qos</code> command which get configured along with the running configs because of auto-qos template.</td>
</tr>
</tbody>
</table>

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).

Configuration Examples for Auto-QoS

**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