Cisco APIC and QoS

New and Changed Information  2
Cisco ACI QoS Overview  2
Cisco ACI QoS Level Settings  5
Custom QoS Policy and Ingress/Egress Markings  9
Class of Service (CoS) Preservation for Ingress and Egress Traffic  13
Multi-Pod QoS and DSCP Translation Policy  15
L3Outs QoS  22
RoCEv2 and the Required APIC QoS Settings  28
Troubleshooting Cisco APIC QoS Policies  33
New and Changed Information

Table 1: New Features and Changed Behavior in Cisco APIC

<table>
<thead>
<tr>
<th>Cisco APIC Release Version</th>
<th>Feature</th>
<th>Description</th>
<th>Where documented</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.0(2)</td>
<td>--</td>
<td>Additional information on QoS behavior in Cisco ACI fabrics.</td>
<td>Cisco ACI QoS Overview</td>
</tr>
<tr>
<td></td>
<td>RoCEv2 QoS</td>
<td>Support for new QoS settings to enable RoCEv2 technology in Cisco APIC environment.</td>
<td>RoCEv2 and the Required APIC QoS Settings</td>
</tr>
<tr>
<td></td>
<td>Custom QoS</td>
<td>Support for additional QoS levels and L3Out configuration.</td>
<td>Custom QoS Policy and Ingress/Egress Markings</td>
</tr>
<tr>
<td></td>
<td>Custom QoS for L3Outs</td>
<td></td>
<td>L3Outs QoS</td>
</tr>
<tr>
<td></td>
<td>Additional QoS priority levels (4, 5, 6)</td>
<td></td>
<td>Multi-Pod QoS and DSCP Translation Policy</td>
</tr>
<tr>
<td></td>
<td>Additional DSCP level for multipod</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>QoS ingress-to-egress markings translation</td>
<td>Support for Cisco ACI fabric to classify the traffic for devices that classify the traffic based only on the CoS value</td>
<td>Custom QoS Policy and Ingress/Egress Markings</td>
</tr>
<tr>
<td>Release 2.1(1)</td>
<td>Multipod QoS</td>
<td>Support for CoS preservation and DSCP Multipod QoS settings was added for multipod topologies.</td>
<td>Multi-Pod QoS and DSCP Translation Policy</td>
</tr>
</tbody>
</table>

Cisco ACI QoS Overview

Cisco ACI Quality of Service (QoS) feature allows you to classify the network traffic in your fabric and then to prioritize and police the traffic flow to help avoid congestion in your network. When traffic is classified within the fabric, it is assigned a QoS Priority Level, which is then used throughout the fabric to provide the most desirable flow of packets through the network.

Any traffic for which the QoS features are enabled undergoes the following stages:

- Classification – identification of the traffic type and assignment of a Cisco ACI QoS Level based on it.
- Policing – control of the traffic based on its classification.
- Marking – tagging of network packets based on the configured policing rules and its behavior.
- Queuing and Scheduling - prioritization and/or isolation of network packets based on their QoS Level and markings.

The following sections provide more detailed information on each of the QoS process flow stages.
Classification and Marking

Traffic classification is used to partition traffic in your Cisco ACI fabric into QoS Levels based on several criteria such as ingress packet headers (DSCP or CoS), source EPGs, or EPG Contracts.

The values used to classify traffic are called match criteria. When you configure a QoS Level for a type of traffic, you can specify one or more of these criteria to match, you can choose to exclude a particular criteria, or you can determine the traffic class by matching any or all criteria. Traffic that fails to match any class is assigned to a default class (Level3) of traffic.

When packets first ingress the Cisco ACI fabric, two values can be use to classify the traffic into the proper QoS Level:

• **Class of Service (CoS):** Also referred to as "dot1p value", a QoS feature developed by the 802.1p group that uses a 3-bit Priority Code Point (PCP) inside the Layer-2 Ethernet frames to differentiate traffic.

• **Differentiated Services Code Point (DSCP):** A Layer-3 alternative to CoS that uses a 6-bit value in the IP packet header to classify traffic.

Marking

After traffic is classified, the packets are marked by adding the QoS class ID to the outer header of each packet. Traffic classification and marking happens on the ingress leaf switches only; the spine and egress leaf switches only map the packets to proper class of service based on the CoS value.

Policing

While Cisco ACI fabrics are non-blocking if properly sized and there are no oversubscription concerns, a leaf interface may still be shared between multiple EPGs. Applying proper QoS policies can prevent one EPG from monopolizing the link.

One of the common use-cases is to classify the traffic coming from a given server to EPGs, for example as data, backup, or vMotion. Following the classification, you can then police the ingress traffic for each EPG to ensure that backup traffic does not consume too much bandwidth and interfere with the data traffic. Using this type of ingress per-EPG policing, we can provision different limits for data EPG, backup EPG, and vMotion EPG on any given leaf switch interface.

When you configure QoS policing in your fabric, the following rules apply:

• The policies can be applied on interfaces or EPGs.

  Interface policies are defined at the tenant level and can be applied in both, ingress and egress directions. Because these policies are attached to a port, they are enforced globally with no concept of individual EPGs.

  EPG policies are defined at the tenant level and can be applied only in the ingress direction. Because these policies are attached to an EPG, they are enforced at the physical interface level per EPG. You can configure a single policer instance to be used by all EPG members or a dedicated policer for each member.

• Policies can be applied from the fabrics access (`infra`) or the tenant (`fvTenant`) portions of the fabric.

• If any traffic exceeds the limits configured in the policies, the packets can be either dropped or marked.

Queuing and Scheduling

After the traffic packets have been classified (or re-classified based on markings) and assigned a QoS Level, they are subject to being queued for transmission. Multiple queues can be used based on the packet's priority and a scheduling algorithm is used to determine which queue's packet is to be transmitted next.

Cisco ACI uses a Deficit Weighted Round Robin (DWRR) scheduling algorithm. This scheduling algorithm allows packets of variable sizes and provides a deficit counter to dynamically adjust queue priorities. The queuing and scheduling policy is a fabric-wide
configuration and applies to all nodes. The same policy is applied within each node whenever packet queuing takes place, which simplifies the configuration and ensures consistent end-to-end compatibility with standard QoS, such as in the NXOS-mode switches.

Cisco ACI fabric supports a number of user-configurable QoS levels as well as levels reserved for fabric control traffic, SPAN, and traceroute traffic. Cisco APIC Release 4.0(1) supports six user-configurable QoS levels, while earlier releases supported three. The table below lists the reserved QoS levels. Each level is mapped to a hardware queue and configured at the fabric level.

<table>
<thead>
<tr>
<th>QoS Group</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>APIC Controller Traffic</td>
<td>Strict priority queue, includes all traffic to and from APIC.</td>
</tr>
<tr>
<td>Control Traffic</td>
<td>Strict priority queue, includes all SUP-generated traffic and control traffic, such as LACP, ISIS, BGP, COOP, ETC.</td>
</tr>
<tr>
<td>SPAN Traffic</td>
<td>Best effort traffic. A Deficit Weighted Round Robin (DWRR) queue with least weight. SPAN and ERSPAN traffic has lower priority than data traffic and will be dropped in case of congestion.</td>
</tr>
<tr>
<td>Traceroute Traffic</td>
<td>Best effort traffic.</td>
</tr>
</tbody>
</table>

Scheduling and Congestion Avoidance

If at any point the network becomes congested, a congestion avoidance algorithm can be used to determine which packets to transmit, queue, or drop. Cisco APIC deploys two different congestion avoidance algorithms for user-configurable QoS Levels:

- **Tail Drop (TD)** – In case of congestion, any new incoming packets (tail end of a queue) are dropped. Tail Drop uses single threshold per queue.

- **Weighted Random Early Detection (WRED)** – Provides an early detection mechanism, which allows for low priority packets to be preemptively dropped in order to protect higher priority queues from congestion. WRED uses one or more thresholds per queue with each queue associated with DSCP or CoS values.

Switch Roles in QoS Flow

When you enable QoS features, the fabric's switches perform the following QoS-related tasks:

<table>
<thead>
<tr>
<th>Switch</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ingress leaf switch</td>
<td>• Classification</td>
</tr>
<tr>
<td></td>
<td>• Marking</td>
</tr>
<tr>
<td></td>
<td>• Buffering</td>
</tr>
<tr>
<td></td>
<td>• Queuing</td>
</tr>
<tr>
<td></td>
<td>• Ingress Policing</td>
</tr>
<tr>
<td>Spine switch</td>
<td>• Buffering</td>
</tr>
<tr>
<td></td>
<td>• Queuing</td>
</tr>
<tr>
<td>Switch</td>
<td>Task</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>Egress leaf switch</td>
<td>• Buffering</td>
</tr>
<tr>
<td></td>
<td>• Queuing</td>
</tr>
<tr>
<td></td>
<td>• Egress Policing</td>
</tr>
</tbody>
</table>

**Cisco ACI QoS Policy Precedence**

Once traffic has been classified, you can use the QoS classes to prioritize flow within your fabric by assigning a QoS level to EPG traffic as described in more detail in the following sections. However, keep in mind that if multiple QoS policies are configured and could apply for any given traffic, only one policy is applied using the following precedence:

- **QoS policy for EPG Contract**
  - If QoS is enabled in the Contract between EPGs, the QoS class specified in the contract is used.

- **QoS policy for source EPG**
  - If QoS is not enabled in the Contract, but custom QoS is enabled at the source EPG level, the custom QoS class is used and traffic is classified based on DSCP or 802.1p values.

- **Default QoS class**
  - If no QoS class is specified, the traffic is assigned Level3 QoS class by default.

**Cisco ACI QoS Level Settings**

Cisco ACI provides a number of user-configurable QoS levels. Cisco APIC Release 4.0(1) supports six user-configurable QoS levels, while earlier releases supported three. The following sections describe how to configure specific settings for each of these levels.

**Configuring Cisco ACI QoS Level Settings Using Cisco APIC GUI**

This section describes how to configure specific settings for each Cisco ACI QoS Level.

**Procedure**

1. From the main menu bar, select **Fabric > Access Policies**.
2. In the left-hand navigation pane, select **Policies > Global > QOS Class > <level>**.

You can configure the following settings for each QoS Level:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin State</td>
<td>The policy administrative state. The state can be:</td>
</tr>
<tr>
<td></td>
<td>• Enabled</td>
</tr>
<tr>
<td></td>
<td>• Disabled</td>
</tr>
<tr>
<td></td>
<td>The default is <strong>Enabled</strong>.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>MTU</td>
<td>The maximum transmission unit for the port. The MTU value can be between 1500 and 9216. The default value is 9216.</td>
</tr>
<tr>
<td>Minimum Buffers</td>
<td>The minimum number of reserved buffers. The number can be between 0 and 3. The default value is 0.</td>
</tr>
<tr>
<td>Congestion Algorithm</td>
<td>The congestion algorithm used for this QoS Level. The congestion algorithm can be:</td>
</tr>
<tr>
<td></td>
<td>• Tail Drop</td>
</tr>
<tr>
<td></td>
<td>• Weighted random early detection</td>
</tr>
<tr>
<td>Congestion Notification</td>
<td>Indicates the state of Explicit Congestion Notification (ECN) setting. Enabling Congestion Notification causes the packets that would be dropped to be ECN-marked instead. The state can be:</td>
</tr>
<tr>
<td></td>
<td>• Enabled</td>
</tr>
<tr>
<td></td>
<td>• Disabled</td>
</tr>
<tr>
<td></td>
<td>The default setting is Disabled. This setting is used for the RoCEv2 feature described in more detail in RoCEv2 and the Required APIC QoS Settings, on page 28.</td>
</tr>
<tr>
<td>Min Threshold (percentage)</td>
<td>The minimum queue threshold as a percentage of the maximum queue length for WRED algorithm. If the average queue size is below the minimum threshold value, the arriving packets are queued immediately. This setting is used for the RoCEv2 feature described in more detail in RoCEv2 and the Required APIC QoS Settings, on page 28.</td>
</tr>
<tr>
<td>Max Threshold (percentage)</td>
<td>The maximum queue threshold as a percentage of the maximum queue length for WRED algorithm. If the average queue size is greater than the maximum threshold value, the arriving packets are dropped. This setting is used for the RoCEv2 feature described in more detail in RoCEv2 and the Required APIC QoS Settings, on page 28.</td>
</tr>
<tr>
<td>Probability (percentage)</td>
<td>The probability value for WRED algorithm.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>(Weighted random early detection algorithm only)</strong></td>
<td>The probability determines whether the packet is dropped or queued when the average queue size is between the minimum and the maximum threshold values. This setting is used for the RoCEv2 feature described in more detail in RoCEv2 and the Required APIC QoS Settings, on page 28.</td>
</tr>
<tr>
<td>Weight</td>
<td>The weight value for WRED algorithm. Weight has a range of 0 to 7 and is used to calculate average queue length. Lower weight prioritizes current queue length, while higher weight prioritizes older queue lengths. This setting is used for the RoCEv2 feature described in more detail in RoCEv2 and the Required APIC QoS Settings, on page 28.</td>
</tr>
<tr>
<td><strong>Scheduling algorithm</strong></td>
<td>The scheduling algorithm used for this QoS Level. The scheduling algorithm can be:</td>
</tr>
<tr>
<td></td>
<td>• Strict priority</td>
</tr>
<tr>
<td></td>
<td>• Weighted round robin</td>
</tr>
<tr>
<td></td>
<td>The default is <strong>Weighted round robin</strong>.</td>
</tr>
<tr>
<td><strong>Bandwidth allocated (in %)</strong></td>
<td>The percentage of total bandwidth allocated to this QoS Level. The value can be between 0 and 100. The default value is 20.</td>
</tr>
<tr>
<td><strong>PFC Admin State</strong></td>
<td>The administrative state of the Priority Flow Control policy applied to FCoE traffic. The state can be:</td>
</tr>
<tr>
<td></td>
<td>• Enabled—enables Priority Flow Control for FCoE traffic.</td>
</tr>
<tr>
<td></td>
<td>• Disabled—disables Priority Flow Control for FCoE traffic.</td>
</tr>
<tr>
<td><strong>No-Drop-CoS</strong></td>
<td>The CoS level to impose no drop FCoE packet handling even in case of FCoE traffic congestion. The options are:</td>
</tr>
<tr>
<td></td>
<td>• cos 0</td>
</tr>
<tr>
<td></td>
<td>• cos 1</td>
</tr>
<tr>
<td></td>
<td>• cos 2</td>
</tr>
<tr>
<td></td>
<td>• cos 3</td>
</tr>
<tr>
<td></td>
<td>• cos 4</td>
</tr>
<tr>
<td></td>
<td>• cos 5</td>
</tr>
<tr>
<td></td>
<td>• cos 6</td>
</tr>
</tbody>
</table>
### Configuring Cisco ACI QoS Level Settings Using NX-OS Style CLI

This section describes how to configure specific settings for each Cisco ACI QoS Level.

**Procedure**

**Step 1** Enter configuration mode.

*Example:*

```
apic1# config
```

**Step 2** Choose the QoS Level you want to configure.

In the following command, replace `level2` with the QoS Level you want to configure:

*Example:*

```
apic1(config)# qos parameters level2
```

**Step 3** Configure one or more settings for the QoS Level.

The following example shows how to configure congestion notification and congestion detection algorithm for a QoS level:

*Example:*

```
apic1(config-qos)# algo wred
apic1(config-qos-algo)# ecn enabled
apic1(config-qos-algo)# maxthreshold 60
apic1(config-qos-algo)# minthreshold 40
apic1(config-qos-algo)# probability 0
apic1(config-qos-algo)# weight 1
apic1(config-qos-algo)# exit
```

The following example shows how to configure no-drop CoS:

*Example:*

```
apic1(config-qos)# pause no-drop cos 1 fabric
apic1(config-qos-algo)#
```
Configuring Cisco ACI QoS Level Settings Using REST API

This section describes how to configure specific settings for each Cisco ACI QoS Level.

Procedure

Configure settings for a QoS Level.

In the following example, replace level2 with the QoS class you want to configure.

POST URL: https://<apic-ip>/api/node/mo/uni.xml

**Example:**

```xml
<qosClass admin="enabled" dn="uni/infra/qosinst-default/class-level2" prio="level2">
    <qosCong algo="wred" wredMaxThreshold="60" wredMinThreshold="40" wredProbability="0" ecn="enabled"/>
    <qosPfcPol name="default" noDropCos="cos0" adminSt="yes" enableScope="fabric"/>
</qosClass>
```

Custom QoS Policy and Ingress/Egress Markings

You can create a custom QoS policy in Cisco APIC by translating the DSCP and CoS values of the ingressing traffic to a QoS priority level to be used inside the Cisco ACI fabric. Translation is supported only if the DSCP values are present in the IP packet and CoS values are present in the Ethernet frames.

For example, this functionality allows the Cisco ACI fabric to classify the traffic for devices that classify the traffic based only on the CoS value, such as Layer-2 packets, which do not have an IP header.

Custom QoS Guidelines and Limitations

If you create custom QoS policies based on both, CoS and DSCP, values and both values are present in an ingressing packet but are matched to different QoS priority levels, the DSCP mapping takes precedence.

Custom QoS policies based on DSCP value translation require 5 continuous chunks of TCAM memory space per DSCP translation policy. If continuous memory space is not available, the DSCP translation policy will fail to program in the hardware and a fault will be generated on the APIC. You can verify available TCAM space using the following command on the switch: `show system internal aclqos qos policy detail`

If you create a custom QoS policy based on CoS value, you must first enable the global fabric CoS preservation policy, as described in Class of Service (CoS) Preservation for Ingress and Egress Traffic, on page 13.

If you are running a release prior to Release 4.0(1), CoS translation is not supported on external L3 interfaces.

CoS translation is supported only if the egress frame is 802.1Q encapsulated.

CoS translation is not supported when the following configuration options are enabled:

- Contracts are configured that include QoS.
- The outgoing interface is on a FEX.
- Multipod QoS using a DSCP policy is enabled.

For more information about Multipod and DSCP policy, see Multi-Pod QoS and DSCP Translation Policy, on page 15.
- Dynamic packet prioritization is enabled.
- If an EPG is configured with intra-EPG endpoint isolation enforced.
- If an EPG is configured with microsegmentation enabled.
- Starting with release 4.0(1), all DPP prioritized traffic has CoS 3 marked in spite of custom QoS configuration.

When these packets are ingressing and egressing same leaf switch, the CoS value is retained, leading to the frames leaving the Fabric with CoS 3 marking.

Creating Custom QoS Policy Using Cisco APIC GUI

This section describes how to create a custom QoS policy and associate it with an EPG using the Cisco APIC GUI.

Before you begin

You must have created the tenant, application, and EPGs that will consume the custom QoS policy.

Procedure

**Step 1** Log in to your Cisco APIC GUI.

**Step 2** From the horizontal navigation bar, select Tenants > <tenant-name>.

**Step 3** In the left-hand navigation pane, expand <tenant-name> > Policies > Protocol > Custom QoS.

**Step 4** Right click the Custom QoS and choose Create Custom QoS Policy.

**Step 5** Provide the name and an optional description of the custom QoS policy information.

**Step 6** Create a DSCP mapping for one or more QoS priority levels.

The DSCP mapping allows you to map ingress DSCP values to a QoS priority level as well as the egress DSCP and CoS value for traffic that leaves the ACI fabric. For each mapping, you can specify the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority</td>
<td>The QoS priority level to which the DSCP values will be mapped.</td>
</tr>
<tr>
<td>DSCP Range From</td>
<td>The start of the DSCP range.</td>
</tr>
<tr>
<td>DSCP Range To</td>
<td>The end of the DSCP range.</td>
</tr>
<tr>
<td>DSCP Target</td>
<td>The DSCP value for egressing traffic.</td>
</tr>
<tr>
<td>Target Cos</td>
<td>The CoS value for the egressing traffic.</td>
</tr>
</tbody>
</table>

**Step 7** Create a CoS mapping for one or more QoS priority levels.

The CoS mapping allows you to map ingress CoS values to a QoS priority level as well as the egress DSCP and CoS value for traffic that leaves the ACI fabric. For each mapping, you can specify the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority</td>
<td>The QoS priority level to which the DSCP values will be mapped.</td>
</tr>
<tr>
<td>Dot1P Range From</td>
<td>The start of the CoS range.</td>
</tr>
<tr>
<td>Dot1P Range To</td>
<td>The end of the CoS range.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>DSCP Target</td>
<td>The DSCP value for egressing traffic.</td>
</tr>
<tr>
<td>Target Cos</td>
<td>The CoS value for the egressing traffic.</td>
</tr>
</tbody>
</table>

**Step 8**  
Click **Submit** to save the changes.

**Step 9**  
Attach the custom QoS policy you created to an EPG.

a) Navigate to **Tenants** > **<tenant-name>** > **Application Profiles** > **<application-profile-name>** > **Application EPGs** > **<application-epg-name>**.

b) In the main window pane, select **Policy** > **General** the custom QoS policy you created.

c) In the main window pane, select the custom QoS policy you created from the **Custom QoS** drop down menu.

d) Click **Submit** to save the changes.

---

**Creating Custom QoS Policy Using NX-OS Style CLI**

This section describes how to create a custom QoS policy and associate it with an EPG using the NX-OS style CLI.

**Before you begin**

You must have created the tenant, application, and EPGs that will consume the custom QoS policy.

**Procedure**

**Step 1**  
Enter configuration mode.

**Example:**
```
apic1# configure
```

**Step 2**  
Enter tenant configuration mode.

**Example:**
```
apic1(config)# tenant <tenant-name>
```

**Step 3**  
Create QoS policy.

**Example:**
```
apic1(config-tenant)# policy-map type qos <qos-policy-name>
```

**Step 4**  
Set DCSP range and target QoS priority level.

**Example:**
```
apic1(config-tenant-pmap-qos)# match dscp AF23 AF31 set-cos 6
```

**Step 5**  
Return to tenant configuration mode.

**Example:**
```
apic1(config-tenant-pmap-qos)# exit
```

---

11
Step 6  Create or edit an application profile.

Example:
apic1(config-tenant)# application <application-name>

Step 7  Create or edit an EPG in the application profile.

To create a normal EPG:

Example:
apic1(config-tenant-app)# epg <epg-name>

To create an external Layer-2 EPG:

Example:
apic1(config-tenant)# external-l2 epg <ext-l2-epg-name>

Step 8  Associate the QoS policy with the EPG.

The system prompt may be different depending on whether you create a normal EPG or an external EPG.

Example:
apic1(config-tenant-app-epg)# service-policy <qos-policy-name>

Step 9  Return to the tenant configuration mode.

Example:
apic1(config-tenant-app-epg)# exit

Creating Custom QoS Policy Using REST API

This section describes how to create a custom QoS policy and associate it with an EPG using the REST API.

Before you begin

You must have created the tenant, application, and EPGs that will consume the custom QoS policy.

Procedure

Step 1  Create a custom QoS policy.

Example:

```
<qosCustomPol name="vrfQos001" dn="uni/tn-t001/qoscustom-vrfQos001">
    <qosDscpClass to="AF31" targetCos="6" target="unspecified" prio="unspecified" from="AF23"/>
    <qosDot1PClass to="1" targetCos="6" target="unspecified" prio="unspecified" from="0"/>
</qosCustomPol>
```

Step 2  Associate the policy with an EPG that will consume it.

Example:

```
<fvAEPg prio="unspecified" prefGrMemb="exclude" pcEnfPref="unenforced" name="ep2" matchT="AtleastOne" isAttrBasedEPg="no" fwdCtrl="" dn="uni/tn-t001/ap-ap2/epg-ep2">
```
Class of Service (CoS) Preservation for Ingress and Egress Traffic

When traffic enters the Cisco ACI fabric, each packet's priority is mapped to a Cisco ACI QoS level. These QoS levels are then stored in the CoS field and DE bit of the packet's outer header while the original headers are discarded.

If you want to preserve the original CoS values of the ingressing packets and restore it when the packet leaves the fabric, you can enable the 802.1p Class of Service (CoS) preservation using a global fabric QoS policy as described in this section.

The CoS preservation is supported in single pod and multipod topologies, however in multipod topologies, CoS preservation can be used only when you are not concerned with preserving the settings in the IPN between pods. To preserve the CoS values of the packets as they are transiting the IPN, use the DSCP translation policy as described in Multi-Pod QoS and DSCP Translation Policy, on page 15.

CoS Preservation Guidelines and Limitations

Only the CoS value within a VLAN header is preserved, the DEI bit is not preserved.

For VXLAN encapsulated packets, the CoS value contained in the outer header is not preserved.

CoS values are not preserved when the following configuration options are enabled:

- Contracts are configured that include QoS.
- The outgoing interface is on a FEX.
- Traffic is flowing from an EPG with isolation enforced to an EPG without isolation enforced.
- A DSCP QoS policy is configured on a VLAN EPG and the packet has an IP header.

DSCP marking can be set at the filter level on the following with the precedence order from the innermost to the outermost:

- Contract
- Subject
- In Term
- Out Term

Note

When specifying vzAny for a contract, external EPG DSCP values are not honored because vzAny is a collection of all EPGs in a VRF and EPG-specific configuration cannot be applied. If EPG-specific target DSCP values are required, then the external EPG should not use vzAny.
Enable Class Of Service (CoS) Preservation Using Cisco APIC GUI

This section describes how to enable CoS preservation to ensure that QoS priority settings are handled the same for traffic entering and transiting a single-pod fabric as for traffic entering one pod and egressing another in a multipod fabric.

---

**Note**
Enabling CoS preservation applies a default CoS-to-DSCP mapping to the various traffic types.

**Procedure**

1. From the main menu bar, select **Fabric > Access Policies**.
2. In the left-hand navigation pane, select **Policies > Global > QOS Class**.
3. In the **Global - QOS Class** main window pane, check the **Preserve COS: Dot1p Preserve** checkbox.
4. Click **Submit** to save the changes.

---

Enable Class Of Service (CoS) Preservation Using NX-OS Style CLI

This section describes how to enable CoS preservation to ensure that QoS priority settings are handled the same for traffic entering and transiting a single-pod fabric as for traffic entering one pod and egressing another in a multipod fabric.

---

**Note**
Enabling CoS preservation applies a default CoS-to-DSCP mapping to the various traffic types.

**Procedure**

1. Enter configuration mode.
   
   **Example:**
   
   ```
   apic1# configure
   ```

2. Enables CoS preservation.
   
   **Example:**
   
   ```
   apic1(config)# qos preserve cos
   ```

---

Enable Class Of Service (CoS) Preservation Using REST API

This section describes how to enable CoS preservation to ensure that QoS priority settings are handled the same for traffic entering and transiting a single-pod fabric as for traffic entering one pod and egressing another in a multipod fabric.
Enabling CoS preservation applies a default CoS-to-DSCP mapping to the various traffic types.

**Procedure**

Enable CoS preservation.

POST https://<apic-ip>/api/node/mo/uni/infra/qosinst-default.xml

Example:

```
<qosInstPol name="default" dn="uni/infra/qosinst-default" ctrl="dot1p-preserve"/>
```

Disable CoS preservation.

Example:

```
<qosInstPol name="default" dn="uni/infra/qosinst-default" ctrl=""/>
```

**Multi-Pod QoS and DSCP Translation Policy**

When traffic is sent and received within the Cisco ACI fabric, the QoS Level is determined based on the CoS value of the VXLAN packet's outer header. In Multi-Pod topologies, where devices that are not under Cisco APIC's management may modify the CoS values in the transiting packets, you can preserve the QoS Level setting by creating a mapping between the Cisco ACI and the DSCP value within the packet.

If you are not concerned with preserving the QoS settings in the IPN traffic between pods, but would like to preserve the original CoS values of the packets ingressing and egressing the fabric, see Class of Service (CoS) Preservation for Ingress and Egress Traffic, on page 13 instead.

*Figure 1: Multi-Pod Topology*

As illustrated in this figure, traffic between pods in a Multi-Pod topology passes through an IPN, which may contain devices that are not under Cisco APIC's management. When a network packet is sent from a spine or a leaf switch in POD1, the devices in the IPN may modify the 802.1p value in the packet. In this case, when the frame reaches a spine or a leaf switch in POD2, it would have an 802.1p value that was assigned by the IPN device, instead of the Cisco ACI QoS Level value assigned at the source in POD1.
In order to preserve the proper QoS Level of the packet and avoid high priority packets from being delayed or dropped, you can use a DSCP translation policy for traffic that goes between multiple PODs connected by an IPN. When a DSCP translation policy is enabled, Cisco APIC converts the QoS Level value (represented by the CoS value of the VXLAN packet) to a DSCP value according to the mapping rules you specify. When a packet sent from POD1 reaches POD2, the mapped DSCP value is translated back into the original CoS value for the appropriate QoS Level.

**DSCP Translation Guidelines**

The following table provides definitions for the DSCP and ToS settings used in DSCP policies and maps.

Prior to Cisco APIC Release 4.0(1), custom DSCP values could be assigned to User Levels 1 through 3. Starting with Cisco APIC Release 4.0(1), values can be selected for Levels 4 through 6 as well.

**Note** For traffic passing through the IPN, do not map any DSCP values to CS6.

<table>
<thead>
<tr>
<th>DSCP or ToS Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AF11</td>
<td>Assured Forwarding Class 1, low probability of dropping</td>
</tr>
<tr>
<td>AF12</td>
<td>Assured Forwarding Class 1, medium probability of dropping</td>
</tr>
<tr>
<td>AF13</td>
<td>Assured Forwarding Class 1, high probability of dropping</td>
</tr>
<tr>
<td>AF21</td>
<td>Assured Forwarding Class 2, low probability of dropping</td>
</tr>
<tr>
<td>AF22</td>
<td>Assured Forwarding Class 2, medium probability of dropping</td>
</tr>
<tr>
<td>AF23</td>
<td>Assured Forwarding Class 2, high probability of dropping</td>
</tr>
<tr>
<td>AF31</td>
<td>Assured Forwarding Class 3, low probability of dropping</td>
</tr>
<tr>
<td>AF32</td>
<td>Assured Forwarding Class 3, medium probability of dropping</td>
</tr>
<tr>
<td>AF33</td>
<td>Assured Forwarding Class 3, high probability of dropping</td>
</tr>
<tr>
<td>AF41</td>
<td>Assured Forwarding Class 4, low probability of dropping</td>
</tr>
<tr>
<td>AF42</td>
<td>Assured Forwarding Class 4, medium probability of dropping</td>
</tr>
<tr>
<td>AF43</td>
<td>Assured Forwarding Class 4, high probability of dropping</td>
</tr>
<tr>
<td>CS0</td>
<td>TOS Class Selector value 0 (the default)</td>
</tr>
<tr>
<td>CS1</td>
<td>TOS Class Selector value 1 (typically used for streaming traffic)</td>
</tr>
<tr>
<td>CS2</td>
<td>TOS Class Selector value 2 (typically used for OAM traffic such as SNMP, SSH, and Syslog)</td>
</tr>
<tr>
<td>CS3</td>
<td>TOS Class Selector value 3 (typically used for signalling traffic)</td>
</tr>
<tr>
<td>CS4</td>
<td>TOS Class Selector value 4 (typically used for Policy Plane traffic and to priority queue)</td>
</tr>
<tr>
<td>DSCP or ToS Level</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>CS5</td>
<td>TOS Class Selector value 5 (typically used for broadcast video traffic)</td>
</tr>
<tr>
<td>CS6</td>
<td>TOS Class Selector value 6 (typically used for Network control traffic)</td>
</tr>
<tr>
<td>CS7</td>
<td>TOS Class Selector value 7</td>
</tr>
<tr>
<td>Expedited Forwarding</td>
<td>EF is dedicated to low-loss, low-latency traffic</td>
</tr>
<tr>
<td>Voice Admit</td>
<td>Similar to EF, but also admitted through CAC</td>
</tr>
</tbody>
</table>

**Creating DSCP Translation Policy Using Cisco APIC GUI**

This section describes how to create a DSCP translation policy to guarantee QoS Level settings across multiple PODs connected by an IPN.

**Procedure**

**Step 1** Navigate to **Tenants > infra**.

**Step 2** In the **Navigation** pane, expand **Policies > Protocol > DSCP class-cos translation policy for L3 traffic**.

**Step 3** In the **Properties** panel, click **Enabled** to enable the DSCP policy.

**Step 4** Map each traffic stream to one of the available levels.

**Note** Each QoS Level must be mapped to a unique value.

**Step 5** Click **Submit** to save the changes.

**Creating DSCP Translation Policy Using NX-OS Style CLI**

This section describes how to create a DSCP translation policy to guarantee QoS Level settings across multiple PODs connected by an IPN.

**Procedure**

**Step 1** Enters configuration mode.

**Example:**

```
apic1# configure
```

**Step 2** Enters tenant configuration mode for the **infra** tenant.

**Example:**

```
apic1(config)# tenant infra
```

**Step 3** Create the DSCP translation map.
**Step 4** Configure the DSCP translation mappings.

**Note** All mappings must be unique within a DSCP translation map and you must not map any QoS level to CS6.

**Example:**

```
apic1(config-qos-cmap)# set dscp-code control CS3
napic1(config-qos-cmap)# set dscp-code span CS5
napic1(config-qos-cmap)# set dscp-code level1 CS0
napic1(config-qos-cmap)# set dscp-code level2 CS1
napic1(config-qos-cmap)# set dscp-code level3 CS2
napic1(config-qos-cmap)# set dscp-code level4 CS3
napic1(config-qos-cmap)# set dscp-code level5 CS4
napic1(config-qos-cmap)# set dscp-code level6 CS5
napic1(config-qos-cmap)# set dscp-code policy CS4
napic1(config-qos-cmap)# set dscp-code traceroute CS5
```

**Step 5** Enable the DSCP translation.

**Example:**

```
apic1(config-qos-cmap)# no shutdown
```

---

**Creating DSCP Translation Policy Using REST API**

This section describes how to create a DSCP translation policy to guarantee QoS Level settings across multiple PODs connected by an IPN.

**Procedure**

**Step 1** Enable and configure a DSCP translation policy.

```
POST https://<apic-ip>/api/node/mo/uni/tn-infra/dscptranspol-default.xml
```

**Example:**

```
<qosDscpTransPol dn="uni/tn-infra/dscptranspol-default" adminSt="enabled" traceroute="AF43" span="AF42" policy="AF22" level3="AF13" level2="AF12" level1="AF11" control="AF21" />
```

**Step 2** Disable the DSCP translation policy.

```
POST https://<apic-ip>/api/node/mo/uni/tn-infra/dscptranspol-default.xml
```

**Example:**

```
<qosDscpTransPol dn="uni/tn-infra/dscptranspol-default" adminSt="disabled" traceroute="AF43" span="AF42" policy="AF22" level3="AF13" level2="AF12" level1="AF11" control="AF21" />
```
Configuring QoS for Multipod

Use this procedure to configure QoS on a multipod setup.

Before you begin

You must have configured Multipod.

Procedure

**Step 1**
Preserve QoS CoS settings to ensure QoS priority settings are handled the same, in APIC traffic through the fabric.

a) On the menu bar, click Fabric > Access Policies.

b) In the Policies pane, expand Global Policies and click QOS Class Policies.

c) In the Global Policies - QOS Class Policies panel, click the Preserve COS Dot1p Preserve check box.

  *Note* By configuring Multipod QoS along with DPP, 802.1p is preserved.

d) Click Submit.

**Step 2**
Match the QoS Class Policy-Level 1, QoS Class Policy-Level 2, and QoS Class Policy-Level 3 according to the policy determined in the IP network (IPN to IPN).

a) On the menu bar, click Fabric > Access Policies.

b) In the Policies pane, click Global Policies > QOS Class Policies > Level 1.

c) In the QOS Class Policy - Level1 panel, update the Scheduling Algorithm and Bandwidth Allocated (in%) drop-down list.

d) Click Submit.

e) Repeat the steps for QoS Class Policy-Level 2 and QoS Class Policy-Level 3.

**Step 3**
Create a DSCP policy to enable guaranteeing QoS priority settings in a multipod topology and configure DSCP mappings for various traffic streams in the fabric.

a) On the menubar, click TENANTS > infra.

b) In the Navigation pane, expand Protocol Policies > DSCP class-cos translation policy for L3 traffic.

c) In the Properties panel, click Enabled to enable the DSCP policy.

d) Map each traffic stream to one of the available levels. They must all be unique.

  *Note* The traffic in the IP network (from IPN to IPN) is treated as priority traffic.

e) Click Submit.

**Example:**
Sample example of DSCP mappings

- User Level 1 traffic is mapped to Expedited Forwarding, since it carries voice and real time traffic.
- User Level 2 traffic is mapped to CS3, as it is often used for traffic marked for precedence 3 treatment.
- User Level 3 traffic is mapped to CS0, as it is the default traffic.
- User Level 4
- User Level 5
- User Level 6
• Control Plane Traffic is mapped with CS7 and to priority queue.

• Policy Plane Traffic is mapped with CS4 and to priority queue.

• Span Traffic is mapped with CS1, as it is traditionally treated as background or scavenger class traffic.

• Traceroute Traffic is mapped with CS5.

Note For traffic passing through the IPN, do not map any DSCP value to CS6.

Step 4 Create class maps to match the markings configured on the APIC.

Example:

class-map type qos match-all UserLevel1
   match dscp 46

class-map type qos match-all UserLevel2
   match dscp 24

class-map type qos match-all UserLevel3
   match dscp 0

class-map type qos match-all SpanTraffic
   match dscp 8

class-map type qos match-all iTraceroute
   match dscp 40

class-map type qos match-all CONTROL-TRAFFIC
   match dscp 48,56

Step 5 Create a policy map to label the ingress Control Plane and Policy Plane traffic with a QoS group.

Example:

policy-map type qos ACI-CLASSIFICATION
   class CONTROL-TRAFFIC
      set qos-group 7
   class UserLevel1
      set qos-group 6
   class UserLevel2
      set qos-group 3
   class UserLevel3
      set qos-group 0

   class SpanTraffic
      set qos-group 1

   class iTraceroute
      set qos-group 5

Step 6 Configure priority queue for the QoS group.

Example:

policy-map type queuing IPN-8q-out-policy
   class type queuing c-out-8q-q7
      priority level 1
   class type queuing c-out-8q-q6
      priority level 2

   class type queuing c-out-8q-q5
      bandwidth remaining percent 0

   class type queuing c-out-8q-q4
      bandwidth remaining percent 0

   class type queuing c-out-8q-q3
      bandwidth remaining percent 40

   class type queuing c-out-8q-q2
      bandwidth remaining percent 0
Step 7  
Apply the policy map to system level QoS.  

**Example:**  
```
system qos
  service-policy type queuing output IPN-8q-out-policy
```

Step 8  
Associate the interfaces connected to the spine switch with the service policy.  

**Example:**  
```
interface Ethernet1/49.4
  description POD2-Spine-401 e1/5
  mtu 9150
  encapsulation dot1q 4
  vrf member IPNACISJC
  service-policy type qos input ACI-CLASSIFICATION
  ip address 10.149.195.106/30
  ip ospf network point-to-point
  ip router ospf IPNACISJC area 0.0.0.0
  ip pim sparse-mode
  ip dhcp relay address 10.0.0.1
  ip dhcp relay address 10.0.0.2
  ip dhcp relay address 10.0.0.3
  no shutdown

interface Ethernet1/50.4
  description POD2-Spine-402 e1/5
  mtu 9150
  encapsulation dot1q 4
  vrf member IPNACISJC
  service-policy type qos input ACI-CLASSIFICATION
  ip address 10.149.195.110/30
  ip ospf network point-to-point
  ip router ospf IPNACISJC area 0.0.0.0
  ip pim sparse-mode
  ip dhcp relay address 10.0.0.1
  ip dhcp relay address 10.0.0.2
  ip dhcp relay address 10.0.0.3
  no shutdown
```

Step 9  
(Optional) Verify the ingress interface on IPN.  
You can verify the ingress interface settings as described in Verifying IPN Ingress Interface Settings, on page 34.

Step 10  
(Optional) Verify the egress interface on IPN.  
You can verify the egress interface settings as described in Verifying IPN Egress Interface Settings, on page 36.
L3Outs QoS

L3Out QoS can be configured using Contracts applied at the external EPG level. Starting with Release 4.0(1), L3Out QoS can also be configured directly on the L3Out interfaces.

**Note** If you are running Cisco APIC Release 4.0(1) or later, we recommend using the custom QoS policies applied directly to the L3Out to configure QoS for L3Outs.

Packets are classified using the ingress DSCP or CoS value so it is possible to use custom QoS policies to classify the incoming traffic into Cisco ACI QoS queues. A custom QoS policy contains a table mapping the DSCP/CoS values to the user queue and to the new DSCP/CoS value (in case of marking). If there is no mapping for a specific DSCP/CoS value, the user queue is selected by the QoS priority setting of the ingress L3Out interface if configured.

L3Outs QoS Guidelines and Limitations

The following guidelines apply to configuring QoS for L3Outs:

- Custom QoS policy is not supported for Layer 3 multicast traffic sourced from outside the ACI fabric (received from L3Out).
- When configuring the QoS policy via contracts to be enforced on the border leaf where the L3Out is located, the VRF instance must be in egress mode (Policy Control Enforcement Direction must be "Egress").
  
  Starting with Release 4.0(1), custom QoS setting can be configured directly on an L3Out and applied for the traffic coming from the border leaf, as such, the VRF does not need to be in egress mode.
- To enable the QoS policy to be enforced, the VRF Policy Control Enforcement Preference must be "Enforced."
- When configuring the Contract that controls communication between the L3Out and other EPGs, include the QoS class or target DSCP in the contract or subject.

**Note** Only configure a QoS class or target DSCP in the contract, not in the external EPG (l3extInstP).

- When creating a contract subject, you must choose a QoS priority level. You cannot choose Unspecified.

**Note** With the exception of Custom QoS Policies as a custom QoS Policy will set the DSCP/CoS value even if the QoS Class is set to Unspecified. When QoS level is unspecified, it by default takes as Level 3 default queue. No unspecified is supported and valid.

- Starting with Release 4.0(1), QoS supports new levels 4, 5, and 6 configured under Global policies, EPG, L3out, custom QoS, and Contracts. The following limitations apply:
  - Number of classes that can be configured with Strict priority is up to 5.
  - The 3 new classes are not supported with non-EX and non-FX switches.
  - If traffic flows between non-EX or non-FX switches and EX or FX switches, the traffic will use QoS level 3.
  - For communicating with FEX for new classes, the traffic carries a Layer 2 COS value of 0.
• Starting with Release 4.0(1), you can configure QoS Class or create a Custom QoS Policy to apply on an L3Out Interface.

**Configuring QoS Directly on L3Out Using GUI**

This section describes how to configure QoS directly on an L3Out. This is the preferred way of configuring L3Out QoS starting with Cisco APIC Release 4.0(1).

**Procedure**

**Step 1**
From the main menu bar, select **Tenants > <tenant-name>**.

**Step 2**
In the left-hand navigation pane, expand **Tenant <tenant-name> > Networking > L3Outs > <routed-network-name> > Logical Node Profiles > <node-profile-name> > Logical Interface Profiles > <interface-profile-name>**.

You may need to create new network, node profile, and interface profile if none exists.

**Step 3**
In the main window pane, configure custom QoS for your L3Out.

You can choose to configure a standard QoS level priority using the **QoS Priority** drop-down list. Alternatively, you can set an existing or create a new custom QoS policy from the **Custom QoS Policy** dropdown.

**Configuring QoS Directly on L3Out Using CLI**

This section describes how to configure QoS directly on an L3Out. This is the preferred way of configuring L3Out QoS starting with Cisco APIC Release 4.0(1).

You can configure QoS for L3Out on one of the following objects:

• Switch Virtual Interface (SVI)

• Sub Interface

• Routed Outside

**Procedure**

**Step 1**
Configure QoS priorities for a L3Out SVI.

**Example:**

```bash
interface vlan 19
  vrf member tenant DT vrf dt-vrf
  ip address 107.2.1.252/24
  description 'SVI19'
  service-policy type qos VrfQos006 // for custom QoS attachment
  set qos-class level6 // for set QoS priority
exit
```

**Step 2**
Configure QoS priorities for a sub-interface.

**Example:**

```bash
interface ethernet 1/48.10
  vrf member tenant DT vrf inter-tentant-ctx2 l3out L4_E48_inter_tennant
```
Step 3  Configure QoS priorities for a routed outside.

**Example:**

```plaintext
interface ethernet 1/37
no switchport
vrf member tenant DT vrf dc-vrf l3out L2E37
ip address 30.1.1.1/24
service-policy type qos vrfQos002
set qos-class level5
exit
```

## Configuring QoS Directly on L3Out Using REST API

This section describes how to configure QoS directly on an L3Out. This is the preferred way of configuring L3Out QoS starting with Cisco APIC Release 4.0(1).

You can configure QoS for L3Out on one of the following objects:

- Switch Virtual Interface (SVI)
- Sub Interface
- Routed Outside

### Procedure

#### Step 1  Configure QoS priorities for a L3Out SVI.

**Example:**

```xml
<l3extLIfP descr="" dn="uni/tn-DT/out-L3_4_E2_24_SVI17/lnodep-L3_4_E2_24/lifp-L3_4_E2_24_SVI_19"
    name="L3_4_E2_24_SVI_19" prio="level6" tag="yellow-green">
    <l3extRsPathL3OutAtt addr="0.0.0.0" autostate="disabled" descr="SVI19" encap="vlan-19"
        encapsScope="local" ifInstT="ext-svi" ipv6Dad="enabled" llAddr="::"
        mac="00:22:BD:F8:19:FF" mode="regular" mtu="inherit"
        tDn="topology/pod-1/protpaths-103-104/pathep-[V_L3_14_2-24]"
        targetDscp="unspecified">
        <l3extMember addr="107.2.1.253/24" ipv6Dad="enabled" llAddr="::" side="B"/>
        <l3extMember addr="107.2.1.252/24" ipv6Dad="enabled" llAddr="::" side="A"/>
    </l3extRsPathL3OutAtt>
    <l3extRsLIfPCustQosPol tnQosCustomPolName="VrfQos006"/>
</l3extLIfP>
```

#### Step 2  Configure QoS priorities for a sub-interface.

**Example:**

```xml
<l3extLIfP dn="uni/tn-DT/out-L4E48_inter_tenant/lnodep-L4E48_inter_tenant/lifp-L4E48"
    name="L4E48" prio="level4" tag="yellow-green">
    <l3extRsPathL3OutAtt addr="210.1.0.254/16" autostate="disabled" encap="vlan-20"
        encapsScope="local" ifInstT="sub-interface" ipv6Dad="enabled" llAddr="::"
        mac="00:22:BD:F8:19:FF" mode="regular" mtu="inherit"
        tDn="topology/pod-1/paths-104/pathep-[eth1/48]" targetDscp="unspecified">
        <l3extRsNdIfPol annotation="" tnNdIfPolName=""/>
    </l3extRsPathL3OutAtt>
</l3extLIfP>
```
Step 3 Configure QoS priorities for a routed outside.

Example:

```xml
<extLIfP dn="uni/tn-DT/out-L2E37/lndep-L2E37/lifp-L2E37OUT"
    name="L2E37OUT" prio="level5" tag="yellow-green">
  <RsPathL3OutAtt addr="30.1.1.1/24" autostate="disabled" encap="unknown"
    encapScope="local" ifInstT="l3-port" ipv6Dad="enabled"
    llAddr="::" mac="00:22:BD:F8:19:FF" mode="regular"
    mtu="inherit" targetDscp="unspecified"
    tDn="topology/pod-1/paths-102/pathep-[eth1/37]"/>
</extLIfP>
```

---

**Configuring QoS Contracts for L3Outs Using Cisco APIC GUI**

This section describes how to configure QoS for L3Outs using Contracts.

**Note**

Starting with Release 4.0(1), we recommend using custom QoS policies for L3Out QoS as described in Configuring QoS Directly on L3Out Using GUI, on page 23 instead.

Configuring QoS classification using a contract as described in this section will take priority over any QoS policies configured directly on the L3Out.

**Procedure**

**Step 1** Configure the VRF instance for the tenant consuming the L3Out to support QoS to be enforced on the border leaf switch that is used by the L3Out.

a) From the main menu bar, choose Tenants > `<tenant-name>`.

b) In the Navigation pane, expand Networking, right-click VRFs, and choose Create VRF.

c) Enter the name of the VRF.

d) In the Policy Control Enforcement Preference field, choose Enforced.

e) In the Policy Control Enforcement Direction choose Egress

   VRF enforcement must be set to Egress when the QoS classification is done in the contract.

f) Complete the VRF configuration according to the requirements for the L3Out.

**Step 2** When configuring filters for contracts to enable communication between the EPGs consuming the L3Out, include a QoS class or target DSCP to enforce the QoS priority in traffic ingressing through the L3Out.

a) On the Navigation pane, under the tenant that that will consume the L3Out, expand Contracts, right-click Filters and choose Create Filter.

b) In the Name field, enter a filter name.

c) In the Entries field, click + to add a filter entry.

d) Add the Entry details, click Update and Submit.

e) Expand the previously created filter and click on a filter entry.
f) Set the **Match DSCP** field to the desired DSCP level for the entry, for example, **EF**.

**Step 3**

Add a contract.

a) Under **Contracts**, right-click **Standard** and choose **Create Contract**.

b) Enter the name of the contract.

c) In the **QoS Class** field, choose the QoS priority for the traffic governed by this contract. Alternatively, you can choose a **Target DSCP** value.

Configuring QoS classification using a contract as described in this section will take priority over any QoS policies configured directly on the L3Out.

d) Click the + icon on **Subjects** to add a subject to the contract.

e) Enter a name for the subject.

f) In the QoS Priority field, choose the desired priority level. You cannot choose **Unspecified**.

g) Under **Filter Chain**, click the + icon on **Filters** and choose the filter you previously created, from the drop down list.

h) Click **Update**.

i) On the **Create Contract Subject** dialog box, click **OK**.

---

### Configuring QoS Contract for L3Out Using NX-OS Style CLI

This section describes how to configure QoS for L3Outs using Contracts.

---

**Note**

Starting with Release 4.0(1), we recommend using custom QoS policies for L3Out QoS as described in Configuring QoS Directly on L3Out Using CLI, on page 23 instead.

---

**Procedure**

---

**Step 1**

Configure the VRF for egress mode and enable policy enforcement to support QoS priority enforcement on the L3Out.

**Example:**

```
api1(config)# configure
api1(config)# tenant t1
api1(config-tenant)# vrf context v1
api1(config-tenant-vrf)# contract enforce egress
api1(config-tenant-vrf)# exit
api1(config-tenant)# exit
api1(config)#
```

**Step 2**

Configure QoS.

When creating filters (**access-list**), include the **match dscp** command with target DSCP level.

When configuring contracts, include the QoS class for traffic ingressing on the L3Out. Alternatively, you can define a target DSCP value. QoS policies are supported on either the contract or the subject.

VRF enforcement must be ingress, for QoS or custom QoS on L3out interface, VRF enforcement need be egress, only when the QOS classification is going to be done in the contract for traffic between EPG and L3out or L3out to L3out.
If QoS classification is set in the contract and VRF enforcement is egress, then contract QoS classification would override the L3Out interface QoS or Custom QoS classification.

**Note**

**Example:**

```
apic1(config)# tenant t1
apic1(config-tenant)# access-list http-filter
apic1(config-tenant-acl)# match ip
apic1(config-tenant-acl)# match tcp dest 80
apic1(config-tenant-acl)# match dscp EF
apic1(config-tenant-acl)# exit
apic1(config-tenant)# contract httpCtrct
apic1(config-tenant-contract)# scope vrf
apic1(config-tenant-contract)# qos-class level1
apic1(config-tenant-contract)# subject http-subject
apic1(config-tenant-contract-subj)# access-group http-filter both
apic1(config-tenant-contract-subj)# exit
apic1(config-tenant)# exit
apic1(config)#
```

---

**Configuring QoS Contract for L3Out Using REST API**

This section describes how to configure QoS for L3Outs using Contracts.

**Note**

Starting with Release 4.0(1), we recommend using custom QoS policies for L3Out QoS as described in Configuring QoS Directly on L3Out Using REST API, on page 24 instead.

**Procedure**

**Step 1**

When configuring the tenant, VRF, and bridge domain, configure the VRF for egress mode (pcEnfDir="egress") with policy enforcement enabled (pcEnfPref="enforced"). Send a post with XML similar to the following example:

**Example:**

```
<fvTenant name="t1">
   <fvCtx name="v1" pcEnfPref="enforced" pcEnfDir="egress"/>
   <fvBD name="bd1">
      <fvRsCtx tnFvCtxName="v1"/>
      <fvSubnet ip="44.44.44.1/24" scope="public"/>
      <fvRsBDToOut tnL3extOutName="l3out1"/>
   </fvBD>
</fvTenant>
```

**Step 2**

When creating the filters and contracts to enable the EPGs participating in the L3Out to communicate, configure the QoS priority.

The contract in this example includes the QoS priority, level1, for traffic ingressing on the L3Out. Alternatively, it could define a target DSCP value. QoS policies are supported on either the contract or the subject.

The filter also has the matchDscp="EF" criteria, so that traffic with this specific TAG received by the L3out processes through the queue specified in the contract subject.
VRF enforcement should be ingress, for QOS or custom QOS on L3out interface, VRF enforcement need be egress, only when the QOS classification is going to be done in the contract for traffic between EPG and L3out or L3out to L3out.

**Note** If QOS classification is set in the contract and VRF enforcement is egress, then contract QOS classification would override the L3out interface QOS or Custom QOS classification. So either we need to configure this one or the new one.

**Example:**

```
<vzFilter name="http-filter">
  <vzEntry name="http-e" etherT="ip" prot="tcp" matchDscp="EF"/>
</vzFilter>
<vzBrCP name="httpCtrct" prio="level1" scope="context">  
  <vzSubj name="subj1">
    <vzRsSubjFiltAtt tnVzFilterName="http-filter"/>
  </vzSubj>
</vzBrCP>
```

---

**RoCEv2 and the Required APIC QoS Settings**

Remote Direct Memory Access (RDMA) over Converged Ethernet (RoCE) technology allows data to be transferred between servers or from storage to server without having to pass through the CPU and main memory path of TCP/IP. The network adapters transfers data directly to and from the application memory bypassing the operating system and the CPU. This zero copy and CPU offloading approach ensures greater CPU availability for other tasks while providing low latency and reduced jitter. A single fabric can be used for both, storage and compute. RoCEv2 provides additional functionality by allowing RDMA to be used with both Layer-2 and Layer-3 (UDP/IP) packets, enabling Layer-3 routing over multiple subnets.

Starting with Cisco Application Policy Infrastructure Controller Release 4.0(1), you can enable RoCEv2 functionality in your fabric by configuring specific QoS options for Layer-3 traffic in Cisco APIC, such as Weighted Random Early Detection (WRED) congestion algorithm and Explicit Congestion Notification (ECN).

The following sections describe how to configure the required QoS options using three different methods – the Cisco APIC GUI, the NX-OS style CLI, and the REST API – but regardless of which you choose, you'll have to configure the following:

- Weighted Random Early Detection (WRED) congestion algorithm, which manages congestion on spine switches using the following configuration options:
  - **WRED Min Threshold** – if the average queue size is below the minimum threshold value, the arriving packets are queued immediately.
  - **WRED Max Threshold** – if the average queue size is greater than the maximum threshold value, the arriving packets are dropped.
  - **WRED Probability** – if the average queue size is between the Min and Max threshold, the Probability value determines whether the packet is dropped or queued.
  - **WRED Weight** – weight has a range of 0 to 7 and is used to calculate average queue length. Lower weight prioritizes current queue length, while higher weight prioritizes older queue lengths.

- Explicit Congestion Notification (ECN), which is used for congestion notification. In case of congestion, ECN gets transmitting device to reduce transmission rate until congestion clears allowing traffic to continue without pause. ECN along with WRED enables end-to-end congestion notification between two endpoints on the network.
• Priority Flow Control (PFC), which is used to achieve Layer 2 flow control. PFC provides the capability to pause traffic in case of congestion.

ROCEv2 Hardware Support.

The following Cisco hardware is supported for ROCEv2 in this release:

• Cisco Nexus 9300-EX platform switches
• Cisco Nexus 9300-FX platform switches
• Cisco Nexus 9300-FX2 platform switches
• N9K-X9700-EX line cards
• N9K-C9504-FM-E fabric modules

Configuring Priority Flow Control (PFC) On Interfaces

Before you can configure the appropriate QoS settings for ROCEv2, you must enable PFC on each interface that is connected to ROCE devices. PFC setting can be set to one of three values, on, off, and auto. If you set it to auto, the DCBX protocol negotiates the PFC state on the interface.

You can configure PFC on one or more interfaces using any of the following methods:

• Using the Cisco APIC GUI, as described in Configuring PFC On Interfaces Using the Cisco APIC GUI, on page 29
• Using the NX-OS style CLI, as described in Configuring PFC On Interfaces Using the NX-OS Style CLI, on page 29
• Using the REST API, as described in Configuring PFC On Interfaces Using the REST API, on page 30

Configuring PFC On Interfaces Using the Cisco APIC GUI

You can use the Cisco APIC GUI to configure PFC state on the interfaces connecting to ROCEv2 devices.

 Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Log in to Cisco APIC.</td>
</tr>
<tr>
<td>Step 2</td>
<td>From the top navigation bar, choose Fabric &gt; Inventory.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the left-hand sidebar, navigate to &lt;pod&gt; &gt; &lt;leaf-switch&gt;.</td>
</tr>
<tr>
<td>Step 4</td>
<td>In the main pane, select the Interface tab.</td>
</tr>
<tr>
<td>Step 5</td>
<td>In the main pane, from the Mode dropdown menu, select Configuration.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Choose an L2 port you want to configure.</td>
</tr>
<tr>
<td>Step 7</td>
<td>In the bottom pane, select the FCoE/FC tab.</td>
</tr>
<tr>
<td>Step 8</td>
<td>Set the PFC State of the port to On.</td>
</tr>
</tbody>
</table>

Configuring PFC On Interfaces Using the NX-OS Style CLI

You can use the NX-OS style CLI to configure PFC state on the interfaces connecting to ROCEv2 devices.
**Procedure**

**Step 1** Enter APIC configuration mode.

*Example:*

```
apic1# config
```

**Step 2** Enter switch configuration.

*Example:*

```
apic1(config)# leaf 101
```

**Step 3** Enable PFC for specific interfaces.

*Example:*

```
apic1(config-leaf)# interface ethernet 1/7-9
apic1(config-leaf-if)# priority-flow-control mode on
```

---

**Configuring PFC On Interfaces Using the REST API**

You can use REST API to configure PFC state on the interfaces connecting to ROCEv2 devices.

**Procedure**

**Step 1** You can configure PFC state on a group of interfaces using a policy group.

*Example:*

```
<polUni>
  <infraInfra>
    <qosPfcIfPol name="testPfcPol1" adminSt="on"/>
    <infraFuncP>
      <infraAccPortGrp name="groupName">
        <infraRsQosPfcIfPol tnQosPfcIfPolName="testPfcPol1"/>
      </infraAccPortGrp>
    </infraFuncP>
  </infraInfra>
</polUni>
```

**Step 2** Alternatively, you can configure PFC state on individual interfaces.

*Example:*

```
<polUni>
  <infraInfra>
    <qosPfcIfPol name="testPfcPol" adminSt="auto"/>
    <infraFuncP>
      <infraAccPortGrp name="testPortG">
        <infraRsQosPfcIfPol tnQosPfcIfPolName="testPfcPol"/>
      </infraAccPortGrp>
    </infraFuncP>
  </infraInfra>
</polUni>
```
Configuring QoS for ROCEv2

After you have enabled PFC on each interface that is connected to ROCE devices, you can configure the appropriate QoS settings for ROCEv2.

You can configure QoS for ROCE using any of the following methods:

- Using the Cisco APIC GUI, as described in Configuring QoS for ROCEv2 Using the GUI, on page 31
- Using the NX-OS style CLI, as described in Configuring QoS for RoCEv2 Using NX-OS Style CLI, on page 32
- Using the REST API, as described in Configuring QoS for RoCEv2 Using REST API, on page 33

Configuring QoS for ROCEv2 Using the GUI

You can use the Cisco APIC GUI to configure the required QoS options to enable support for RoCEv2 in your fabric.

Procedure

Step 1 Log in to Cisco APIC.
Step 2 Navigate to Fabric > Access Policies > Policies > Global > QOS Class
Step 3 Select the QOS Class Level for which you want to configure ROCEv2
Step 4 For the Congestion Algorithm option, select Weighted random early detection.
Step 5 For the Congestion Notification option, select Enabled. Enabling Congestion Notification causes the packets that would be dropped to be ECN-marked instead.
Step 6 For the Min Threshold (percentage) option, set the minimum queue threshold as a percentage of the maximum queue length.
   If the average queue size is below the minimum threshold value, the arriving packets are queued immediately.
Step 7 For the Max Threshold (percentage) option, set the maximum queue threshold as a percentage of the maximum queue length.
   If the average queue size is greater than the maximum threshold value, the arriving packets are dropped or marked if ECN is enabled.
Step 8 For the Probability (percentage) option, set the probability value.
   The probability determines whether the packet is dropped or queued when the average queue size is between the minimum and the maximum threshold values.
Step 9 For the Weight option, set the weight value.
   Weight has a range of 0 to 7 and is used to calculate average queue length. Lower weight prioritizes current queue length, while higher weight prioritizes older queue lengths.
Step 10 Check the PFC Admin State checkbox and specify a value for the No-Drop-CoS option to be used by PFC.
Step 11 For the **Scope** option, select *Fabric-wide PFC.*

Step 12 Optionally, you can choose to enable the **Forward Non-ECN Traffic** option, so that non-ECN traffic is not dropped even when the queue is congested. **Congestion Notification** must be enabled for this option to be configurable.

---

**Configuring QoS for RoCEv2 Using NX-OS Style CLI**

You can use the NX-OS style CLI to configure the required QoS options to enable support for RoCEv2 in your fabric.

**Procedure**

---

**Step 1** Enter configuration mode.

**Example:**

```
apic1# config
```

**Step 2** Choose the QoS Level you want to configure.

In the following command, replace *level2* with the QoS Level you want to configure:

**Example:**

```
apic1(config)# qos parameters level2
```

**Step 3** Configure the congestion algorithm and its parameters.

**Example:**

```
apic1(config-qos)# algo wred
apic1(config-qos-algo)# ecn enabled
apic1(config-qos-algo)# maxthreshold 60
apic1(config-qos-algo)# minthreshold 40
apic1(config-qos-algo)# probability 0
apic1(config-qos-algo)# weight 1
apic1(config-qos-algo)# exit
```

**Step 4** (Optional) Configure forwarding of the non-ECN traffic.

You can choose to enable forwarding of all non-ECN traffic, even when the queue is congested.

**Example:**

```
apic1(config-qos-algo)# fwdnonecn enabled
```

**Step 5** Exit congestion algorithm configuration.

**Example:**

```
apic1(config-qos-algo)# exit
```

**Step 6** Configure the CoS value for the QoS Level you chose.

**Example:**

```
apic1(config-qos)# pause no-drop cos 4 fabric
```

If you do not provide the *fabric* parameter, the default value is set to TOR.
Configuring QoS for RoCEv2 Using REST API

You can use REST API to configure the required QoS options to enable support for RoCEv2 in your fabric.

Procedure

Step 1  Configure QoS for RoCEv2.

In the following example, replace `level2` with the QoS class you want to configure and the WRED parameters with values appropriate for your environment.

**POST URL:** https://<apic-ip>/api/node/mo/uni.xml

**Example:**

```xml
<qosClass admin="enabled" dn="uni/infra/qosinst-default/class-level2" prio="level2">
    <qosCong algo="wred" wredMaxThreshold="60" wredMinThreshold="40" wredProbability="0"
        ecn="enabled"/>
    <qosPfcPol name="default" noDropCos="cos0" adminSt="yes" enableScope="fabric"/>
</qosClass>
```

Step 2  (Optional) Configure forwarding of the non-ECN traffic.

You can choose to enable forwarding of all non-ECN traffic, even when the queue is congested.

**Example:**

```xml
<qosInstPol dn="uni/infra/qosinst-default" FabricFlushInterval=450 FabricFlushSt="yes">
</qosInstPol>
```

Troubleshooting Cisco APIC QoS Policies

The following table summarizes common troubleshooting scenarios for Cisco APIC QoS.

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
</table>
| Unable to update a configured QoS policy. | 1. Invoke the following API to ensure that qospDscpRule is present on the leaf.  
   GET https://192.0.20.123/api/node/class/qospDscpRule.xml  
2. Ensure that the QoS rules are accurately configured and associated to the EPG ID to which the policy is attached.  
   Use the following NX-OS style CLI commands to verify the configuration.  
   ```
   leaf1# show vlan  
   leaf1# show system internal aclqos qos policy detail  
   apic1# show running-config tenant tenant-name policy-map type qos  
   custom-qos-policy-name  
   apic1# show running-config tenant tenant-name application application-name  
   epg epg-name  
   ``` |
**Problem**
Show QoS interface statistics.

**Solution**
CLI displays statistics for eth1/1 for only QoS classes – level1, leve2, level3, level4, level5, level6, and policy-plane – if you don’t use “detail” option.

NXOS ibash cli:
tor-leaf1# show queuing interface ethernet 1/1 [detail]

If you want to display statistics for control-plane and span classes for an interface, you need to use CLI with the “detail” option.

Example: fabric 107 show queuing interface ethernet 1/1 detail

APIC CLI:
swtbl123-lfc1# fabric node_id show queuing interface ethernet 1/1

---

**Verifying IPN Ingress Interface Settings**

This section describes how to verify the IPN ingress interface settings you have configured in Configuring QoS for Multipod, on page 19.

IPNFOD2# show policy-map interface ethernet 1/50.4 input

Global statistics status: enabled

Ethernet1/50.4

Service-policy (qos) input: ACI-CLASSIFICATION
SNMP Policy Index: 285215377

Class-map (qos): CONTROL-TRAFFIC (match-all)

<table>
<thead>
<tr>
<th>Slot 1</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1434 packets</td>
<td></td>
</tr>
<tr>
<td>Aggregate forwarded:</td>
<td>1434</td>
</tr>
<tr>
<td>Match: dscp 48,56</td>
<td></td>
</tr>
<tr>
<td>set qos-group 7</td>
<td></td>
</tr>
</tbody>
</table>

Class-map (qos): UserLevel1 (match-all)
Aggregate forwarded: 0 packets
Match: dscp 46
set qos-group 6

Class-map (qos): UserLevel2 (match-all)
Aggregate forwarded: 0 packets
Match: dscp 24
set qos-group 3

Class-map (qos): UserLevel3 (match-all)

<table>
<thead>
<tr>
<th>Slot 1</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>25 packets</td>
<td></td>
</tr>
<tr>
<td>Aggregate forwarded:</td>
<td>25</td>
</tr>
<tr>
<td>Match: dscp 0</td>
<td></td>
</tr>
<tr>
<td>set qos-group 0</td>
<td></td>
</tr>
</tbody>
</table>

Class-map (qos): SpanTraffic (match-all)
Aggregate forwarded: 34
0 packets
Match: dscp 8
set qos-group 1

Class-map (qos): iTraceroute (match-all)
Aggregate forwarded :
0 packets
Match: dscp 40
set qos-group 5

IPNPOD2# show policy-map interface ethernet 1/49.4 input
Global statistics status: enabled

Ethernet1/49.4
Global statistics status: enabled
Ethernet1/49.4

Service-policy (qos) input: ACI-CLASSIFICATION
SNMP Policy Index: 285215373

Class-map (qos): CONTROL-TRAFFIC (match-all)
Slot 1
5149 packets
Aggregate forwarded :
5149 packets
Match: dscp 48,56
set qos-group 7

Class-map (qos): UserLevel1 (match-all)
Aggregate forwarded :
0 packets
Match: dscp 46
set qos-group 6

Class-map (qos): UserLevel2 (match-all)
Aggregate forwarded :
0 packets
Match: dscp 24
set qos-group 3

Class-map (qos): UserLevel3 (match-all)
Slot 1
960 packets
Aggregate forwarded :
960 packets
Match: dscp 0
set qos-group 0

Class-map (qos): SpanTraffic (match-all)
Aggregate forwarded :
0 packets
Match: dscp 8
set qos-group 1

Class-map (qos): iTraceroute (match-all)
Aggregate forwarded :
0 packets
Match: dscp 40
Verifying IPN Egress Interface Settings

This section describes how to verify the IPN egress interface settings you have configured in Configuring QoS for Multipod, on page 19.

```
IPNP0D1# show queuing interface e 1/3 | b "GROUP 7"
```

---

### Egress Queuing for Ethernet 1/3 [System]

<table>
<thead>
<tr>
<th>QoS-Group#</th>
<th>Bandwidth%</th>
<th>PrioLevel</th>
<th>Shape</th>
<th>QLimit</th>
<th>Min</th>
<th>Max</th>
<th>Units</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>-</td>
<td>1</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>9(D)</td>
</tr>
<tr>
<td>6</td>
<td>-</td>
<td>2</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>9(D)</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>9(D)</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>9(D)</td>
</tr>
<tr>
<td>3</td>
<td>20</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>9(D)</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>9(D)</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>9(D)</td>
</tr>
<tr>
<td>0</td>
<td>59</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>9(D)</td>
</tr>
</tbody>
</table>

---

**QOS GROUP 0**

- **Unicast**
  - Tx Pkts: 125631
  - Tx Byts: 42902871
- WRED/AFD & Tail Drop Pkts: 0
- WRED/AFD & Tail Drop Byts: 0
- WD & Tail Drop Pkts: 0
- Q Depth Byts: 0

**QOS GROUP 1**

- **Unicast**
  - Tx Pkts: 0
  - Tx Byts: 0
- WRED/AFD & Tail Drop Pkts: 0
- WRED/AFD & Tail Drop Byts: 0
- WD & Tail Drop Pkts: 0
- Q Depth Byts: 0

**QOS GROUP 2**

- **Unicast**
  - Tx Pkts: 0
  - Tx Byts: 0
- WRED/AFD & Tail Drop Pkts: 0
- WRED/AFD & Tail Drop Byts: 0
- WD & Tail Drop Pkts: 0
- Q Depth Byts: 0

**QOS GROUP 3**

- **Unicast**
  - Tx Pkts: 0
  - Tx Byts: 0
- WRED/AFD & Tail Drop Pkts: 0
- WRED/AFD & Tail Drop Byts: 0
- WD & Tail Drop Pkts: 0
- Q Depth Byts: 0

---

set qos-group 5
<table>
<thead>
<tr>
<th></th>
<th>Unicast</th>
<th>Multicast</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tx Pkts</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Tx Byts</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>WRED/AFD &amp; Tail Drop Pkts</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>WRED/AFD &amp; Tail Drop Byts</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Q Depth Byts</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>WD &amp; Tail Drop Pkts</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

| QOS GROUP 4 |
|------------------|---------|-----------|
| Tx Pkts          | 0       | 0         |
| Tx Byts          | 0       | 0         |
| WRED/AFD & Tail Drop Pkts | 0 | 0 |
| WRED/AFD & Tail Drop Byts | 0 | 0 |
| Q Depth Byts     | 0       | 0         |
| WD & Tail Drop Pkts | 0 | 0 |

| QOS GROUP 5 |
|------------------|---------|-----------|
| Tx Pkts          | 0       | 0         |
| Tx Byts          | 0       | 0         |
| WRED/AFD & Tail Drop Pkts | 0 | 0 |
| WRED/AFD & Tail Drop Byts | 0 | 0 |
| Q Depth Byts     | 0       | 0         |
| WD & Tail Drop Pkts | 0 | 0 |

| QOS GROUP 6 |
|------------------|---------|-----------|
| Tx Pkts          | 645609  | 217       |
| Tx Byts          | 115551882 | 25606    |
| WRED/AFD & Tail Drop Pkts | 0 | 0 |
| WRED/AFD & Tail Drop Byts | 0 | 0 |
| Q Depth Byts     | 0       | 0         |
| WD & Tail Drop Pkts | 0 | 0 |

| QOS GROUP 7 |
|------------------|---------|-----------|
| Tx Pkts          | 23428   | 9         |
| Tx Byts          | 4132411 | 1062      |
| WRED/AFD & Tail Drop Pkts | 0 | 0 |
| WRED/AFD & Tail Drop Byts | 0 | 0 |
| Q Depth Byts     | 0       | 0         |
| WD & Tail Drop Pkts | 0 | 0 |

| CONTROL QOS GROUP |
|-------------------|---------|-----------|
| Tx Pkts          | 6311    | 0         |
| Tx Byts          | 809755  | 0         |
| Tail Drop Pkts   | 0       | 0         |
| Tail Drop Byts   | 0       | 0         |
| WD & Tail Drop Pkts | 0 | 0 |

| SPAN QOS GROUP |
|-----------------|---------|-----------|

37
<table>
<thead>
<tr>
<th>Unicast</th>
<th>Multicast</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tx Pkts</td>
<td>0</td>
</tr>
<tr>
<td>Tx Byts</td>
<td>0</td>
</tr>
<tr>
<td>Tail Drop Pkts</td>
<td>0</td>
</tr>
<tr>
<td>Tail Drop Byts</td>
<td>0</td>
</tr>
<tr>
<td>WD &amp; Tail Drop Pkts</td>
<td>0</td>
</tr>
</tbody>
</table>

**Ingress Queuing for Ethernet1/3**

---

**QoS-Group**

<table>
<thead>
<tr>
<th>Pause</th>
<th>Buff Size</th>
<th>Pause Th</th>
<th>Resume Th</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>6</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>5</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>4</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>3</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>2</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>1</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>0</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

**Per Port Ingress Statistics**

- Hi Priority Drop Pkts: 0
- Low Priority Drop Pkts: 0
- Ingress Overflow Drop Pkts: 0

**PFC Statistics**

---

**Egress Queuing for Ethernet1/4 [System]**

---

<table>
<thead>
<tr>
<th>QoS-Group#</th>
<th>Bandwidth%</th>
<th>PriLevel</th>
<th>Shape</th>
<th>QLimit</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Min</td>
<td>Max</td>
<td>Units</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>1</td>
<td>-</td>
<td>-</td>
<td>9 (D)</td>
</tr>
<tr>
<td>6</td>
<td>2</td>
<td>-</td>
<td>-</td>
<td>9 (D)</td>
</tr>
<tr>
<td>QOS GROUP 0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>+-------------------------------------------------------------+</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Unicast</td>
<td>Multicast</td>
<td></td>
<td></td>
</tr>
<tr>
<td>+-------------------------------------------------------------+</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tx Pkts</td>
<td>63049</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tx Byts</td>
<td>15968783</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WRED/AFD &amp; Tail Drop Pkts</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WRED/AFD &amp; Tail Drop Byts</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Q Depth Byts</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WD &amp; Tail Drop Pkts</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>QOS GROUP 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>+-------------------------------------------------------------+</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Unicast</td>
<td>Multicast</td>
<td></td>
<td></td>
</tr>
<tr>
<td>+-------------------------------------------------------------+</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tx Pkts</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tx Byts</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WRED/AFD &amp; Tail Drop Pkts</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WRED/AFD &amp; Tail Drop Byts</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Q Depth Byts</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WD &amp; Tail Drop Pkts</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>QOS GROUP 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>+-------------------------------------------------------------+</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Unicast</td>
<td>Multicast</td>
<td></td>
<td></td>
</tr>
<tr>
<td>+-------------------------------------------------------------+</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tx Pkts</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tx Byts</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WRED/AFD &amp; Tail Drop Pkts</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WRED/AFD &amp; Tail Drop Byts</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Q Depth Byts</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WD &amp; Tail Drop Pkts</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>QOS GROUP 3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>+-------------------------------------------------------------+</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Unicast</td>
<td>Multicast</td>
<td></td>
<td></td>
</tr>
<tr>
<td>+-------------------------------------------------------------+</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tx Pkts</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tx Byts</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WRED/AFD &amp; Tail Drop Pkts</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WRED/AFD &amp; Tail Drop Byts</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Q Depth Byts</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WD &amp; Tail Drop Pkts</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>QOS GROUP 4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>+-------------------------------------------------------------+</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Unicast</td>
<td>Multicast</td>
<td></td>
<td></td>
</tr>
<tr>
<td>+-------------------------------------------------------------+</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tx Pkts</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tx Byts</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WRED/AFD &amp; Tail Drop Pkts</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WRED/AFD &amp; Tail Drop Byts</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Q Depth Byts</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WD &amp; Tail Drop Pkts</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>QOS GROUP 5</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>+-------------------------------------------------------------+</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Unicast</td>
<td>Multicast</td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
<td>-----------</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Tx Pkts</strong></td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Tx Byts</strong></td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WRED/AFD &amp; Tail Drop Pkts</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WRED/AFD &amp; Tail Drop Byts</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Q Depth Byts</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WD &amp; Tail Drop Pkts</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**QOS GROUP 6**

<table>
<thead>
<tr>
<th></th>
<th>Unicast</th>
<th>Multicast</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Tx Pkts</strong></td>
<td>1141418</td>
<td>0</td>
</tr>
<tr>
<td><strong>Tx Byts</strong></td>
<td>23770324</td>
<td>0</td>
</tr>
<tr>
<td>WRED/AFD &amp; Tail Drop Pkts</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>WRED/AFD &amp; Tail Drop Byts</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Q Depth Byts</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>WD &amp; Tail Drop Pkts</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

**QOS GROUP 7**

<table>
<thead>
<tr>
<th></th>
<th>Unicast</th>
<th>Multicast</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Tx Pkts</strong></td>
<td>32440</td>
<td>0</td>
</tr>
<tr>
<td><strong>Tx Byts</strong></td>
<td>6986806</td>
<td>0</td>
</tr>
<tr>
<td>WRED/AFD &amp; Tail Drop Pkts</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>WRED/AFD &amp; Tail Drop Byts</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Q Depth Byts</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>WD &amp; Tail Drop Pkts</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

**CONTROL QOS GROUP**

<table>
<thead>
<tr>
<th></th>
<th>Unicast</th>
<th>Multicast</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Tx Pkts</strong></td>
<td>6275</td>
<td>0</td>
</tr>
<tr>
<td><strong>Tx Byts</strong></td>
<td>804748</td>
<td>0</td>
</tr>
<tr>
<td>Tail Drop Pkts</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Tail Drop Byts</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>WD &amp; Tail Drop Pkts</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

**SPAN QOS GROUP**

<table>
<thead>
<tr>
<th></th>
<th>Unicast</th>
<th>Multicast</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Tx Pkts</strong></td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td><strong>Tx Byts</strong></td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Tail Drop Pkts</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Tail Drop Byts</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>WD &amp; Tail Drop Pkts</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Ingress Queuing for Ethernet1/4

---

<table>
<thead>
<tr>
<th>QoS-Group#</th>
<th>Buff Size</th>
<th>Pause Pause Th</th>
<th>Resume Th</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>6</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>5</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>4</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>3</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>2</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>
Per Port Ingress Statistics

- Hi Priority Drop Pkts: 0
- Low Priority Drop Pkts: 0
- Ingress Overflow Drop Pkts: 0

PFC Statistics

<table>
<thead>
<tr>
<th>PFC_CoS</th>
<th>QOS Group</th>
<th>TxPause</th>
<th>TxCount</th>
<th>RxPause</th>
<th>RxCount</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Inactive</td>
<td>0</td>
<td>0</td>
<td>Inactive</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>Inactive</td>
<td>0</td>
<td>0</td>
<td>Inactive</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>Inactive</td>
<td>0</td>
<td>0</td>
<td>Inactive</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>Inactive</td>
<td>0</td>
<td>0</td>
<td>Inactive</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>Inactive</td>
<td>0</td>
<td>0</td>
<td>Inactive</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>Inactive</td>
<td>0</td>
<td>0</td>
<td>Inactive</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>Inactive</td>
<td>0</td>
<td>0</td>
<td>Inactive</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td>Inactive</td>
<td>0</td>
<td>0</td>
<td>Inactive</td>
<td>0</td>
</tr>
<tr>
<td>Americas Headquarters</td>
<td>Asia Pacific Headquarters</td>
<td>Europe Headquarters</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----------------------</td>
<td>--------------------------</td>
<td>---------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>San Jose, CA 95134-1706 USA</td>
<td>Singapore</td>
<td>Amsterdam, The Netherlands</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.