Cisco Nexus 3400-S NX-OS QoS Configuration Guide, Release 9.3(x)

First Published: 2019-12-23

Last Modified: 2020-08-20

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

Preface

This preface includes the following sections:

Audience

This publication is for network administrators who install, configure, and maintain Cisco Nexus switches.

Document Conventions

Command descriptions use the following conventions:

Convention	Description
bold	Bold text indicates the commands and keywords that you enter literally as shown.
Italic	Italic text indicates arguments for which the user supplies the values.
[x]	Square brackets enclose an optional element (keyword or argument).
[x | y]	Square brackets enclosing keywords or arguments separated by a vertical bar indicate an optional choice.
{x | y}	Braces enclosing keywords or arguments separated by a vertical bar indicate a required choice.
[x {y | z}]	Nested set of square brackets or braces indicate optional or required choices within optional or required elements. Braces and a vertical bar within square brackets indicate a required choice within an optional element.

Convention	Description
`variable`	Indicates a variable for which you supply values, in context where italics cannot be used.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.

Examples use the following conventions:

Convention	Description
`screen font`	Terminal sessions and information the switch displays are in screen font.
`boldface screen font`	Information you must enter is in boldface screen font.
italic screen font	Arguments for which you supply values are in italic screen font.
< >	Nonprinting characters, such as passwords, are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Related Documentation for Cisco Nexus 3000 Series Switches

The entire Cisco Nexus 3000 Series switch documentation set is available at the following URL:

https://www.cisco.com/c/en/us/support/switches/nexus-3000-series-switches/tsd-products-support-series-home.html

Documentation Feedback

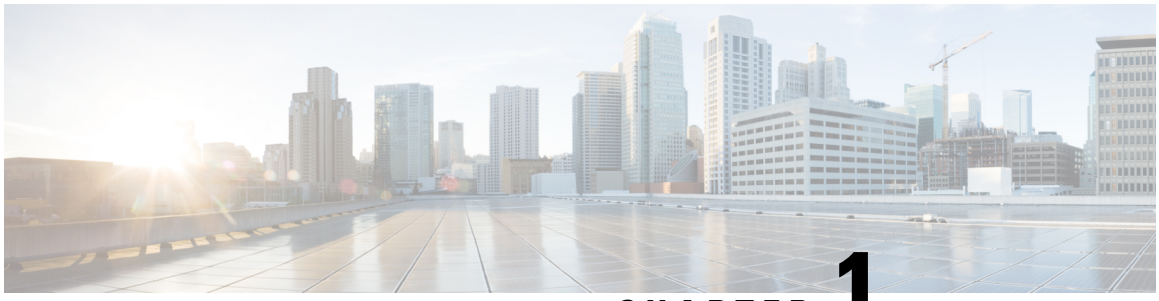
To provide technical feedback on this document, or to report an error or omission, please send your comments to nexus3k-docfeedback@cisco.com. We appreciate your feedback.

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.



CHAPTER 1

New and Changed Information

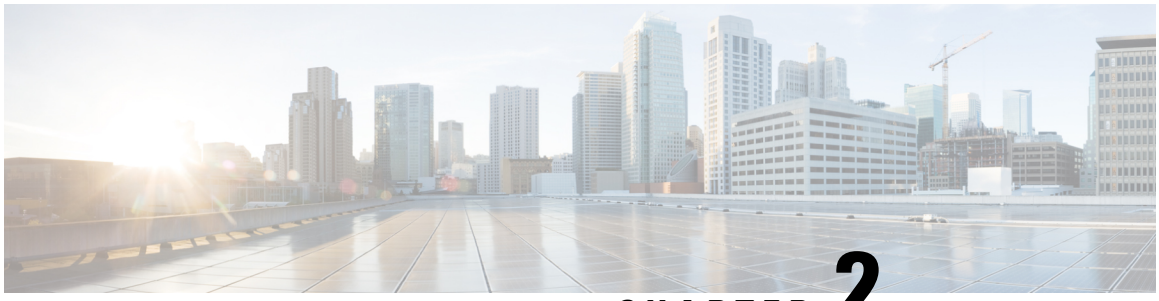
This chapter contains the following sections:

New and Changed Information

The following table provides a list of the significant new and changed features in this release, and links to the corresponding information added to this guide. The table does not provide an exhaustive list of all the changes in this guide or the release.

Feature	Description	Added or Changed in Release	Where Documented
Dynamic Buffer Sharing	Support for configuring drop and no-drop buffer sharing within a slice.	9.3(4)	Managing Dynamic Buffer Sharing, on page 84
New guide	First publication of Cisco Nexus 3400-S Quality of Service Configuration Guide for release 9.3(x).	9.3(3)	

New and Changed Information



CHAPTER 2

Overview

About QoS Features

You use the QoS features to provide the most desirable flow of traffic through a network. QoS allows you to classify the network traffic, police and prioritize the traffic flow, and help avoid traffic congestion in a network. The control of traffic is based on the fields in the packets that flow through the system. You use the Modular QoS (MQC) CLI to create the traffic classes and policies of the QoS features.

QoS features are applied using QoS and queuing policies as follows:

- QoS policies include classification and marking features.
- QoS policies include policing features.
- QoS policies include shaping, weighted random early detection (WRED), and explicit congestion notification (ECN) features.
- Queuing policies use the queuing and scheduling features.

Note The system-defined QoS features and values that are discussed in the "Using Modular QoS CLI" section apply globally to the entire device and cannot be modified.

Using QoS

Traffic is processed based on how you classify it and the policies that you create and apply to traffic classes.

To configure QoS features, you use the following steps:

1. Create traffic classes by classifying the incoming packets that match criteria such as IP address or QoS fields.
2. Create policies by specifying actions to take on the traffic classes, such as policing, marking, or dropping packets.
3. Apply policies to a port, port channel, or subinterface.

You use MQC to create the traffic classes and policies of the QoS features.

Note The queuing and scheduling operations of the overall QoS feature are applicable to both IPv4 and IPv6.

Note IP tunnels do not support access control lists (ACLs) or QoS policies.

Classification

You use classification to partition traffic into classes. You classify the traffic based on the port characteristics or the packet header fields that include IP precedence, differentiated services code point (DSCP), Layer 3 to Layer 4 parameters, and the packet length.

The values used to classify traffic are called match criteria. When you define a traffic class, you can specify multiple match criteria, you can choose to not match on a particular criterion, 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 of traffic called class-default.

Marking

Marking is the setting of QoS information that is related to a packet. You can set the value of a standard QoS field for COS, IP precedence and DSCP, and internal labels (such as QoS groups) that can be used in subsequent actions. Marking QoS groups is used to identify the traffic type for queuing and scheduling traffic.

Policing

Policing is the monitoring of data rates for a particular class of traffic. The device can also monitor associated burst sizes.

Single-rate policers monitor the specified committed information rate (CIR) of traffic. Dual-rate policers monitor both CIR and peak information rate (PIR) of traffic.

Queuing and Scheduling

The queuing and scheduling process allows you to control the bandwidth allocated to traffic classes so that you achieve the desired trade-off between throughput and latency.

You can apply weighted random early detection (WRED) to a class of traffic, which allows packets to be dropped based on the QoS group. The WRED algorithm allows you to perform proactive queue management to avoid traffic congestion.

You can shape traffic by imposing a maximum data rate on a class of traffic so that excess packets are retained in a queue to smooth (constrain) the output rate. In addition, minimum bandwidth shaping can be configured to provide a minimum guaranteed bandwidth for a class of traffic.

You can limit the size of the queues for a particular class of traffic by applying either static or dynamic limits.

ECN can be enabled along with WRED on a particular class of traffic to mark the congestion state instead of dropping the packets.

Sequencing of QoS Actions

The following are the three types of policies:

- **network qos**—Defines the characteristics of QoS properties network wide.
- **qos**—Defines MQC objects that you can use for marking and policing.
- **queuing**—Defines MQC objects that you can use for queuing and scheduling.

Note The default type of policy is **qos**.

The system performs actions for QoS policies only if you define them under the type qos service policies.

Sequencing of Ingress Traffic Actions

The sequence of QoS actions on ingress traffic is as follows:

1. Classification
2. Marking
3. Policing

Sequencing of Egress Traffic Actions

The sequencing of QoS actions on egress traffic is as follows:

1. Queuing and scheduling

High Availability Requirements for QoS Features

The Cisco NX-OS QoS software recovers its previous state after a software restart, and it is capable of a switchover from the active supervisor to the standby supervisor without a loss of state.

QoS Feature Configuration with MQC

You use MQC to configure QoS features. The MQC configuration commands are shown in the following table:

Table 1: MQC Configuration Commands

MQC Command	Description
class-map	Defines a class map that represents a class of traffic.
policy-map	Defines a policy map that represents a set of policies to be applied to a set of class maps.

You can modify or delete MQC objects, except system-defined objects, when the objects are not associated with any interfaces.

After a QoS policy is defined, you can attach the policy map to an interface by using the interface configuration command shown in the following table:

Table 2: Interface Command to Attach a Policy Map to an Interface

Interface Command	Description
service-policy	Applies the specified policy map to input or output packets on the interface.

QoS Statistics

Statistics are maintained for each policy, class action, and match criteria per interface. You can enable or disable the collection of statistics, you can display statistics using the **show policy-map** interface command, and you can clear statistics based on an interface or policy map with the **clear qos statistics** command. Statistics are enabled by default and can be disabled globally.

Default QoS Behavior

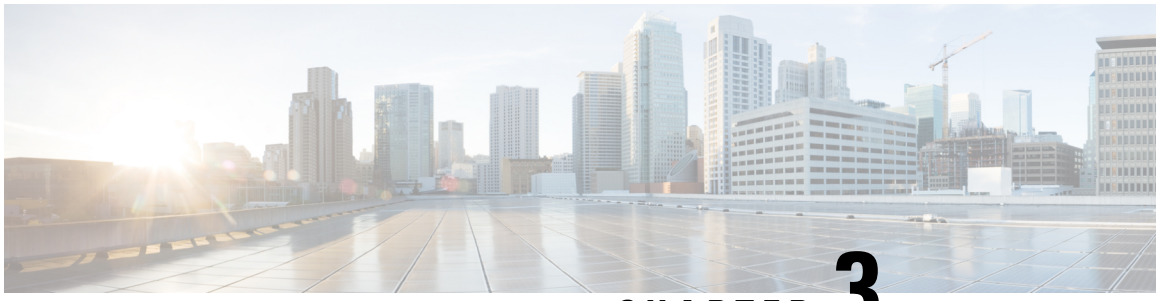
The QoS queuing features are enabled by default. Specific QoS-type features, such as policing and marking, are enabled only when a policy is attached to an interface. Specific policies are enabled when that policy is attached to an interface.

By default, the device always enables a system default queuing policy, or system-defined queuing policy map, on each port and port channel. When you configure a queuing policy and apply the new queuing policy to specified interfaces, the new queuing policy replaces the default queuing policy, and those rules now apply.

The device enables other QoS features, policing and marking, only when you apply a policy map to an interface.

Virtual Device Contexts

Cisco NX-OS can segment operating system and hardware resources into virtual device contexts (VDCs) that emulate virtual devices. The Cisco Nexus 3400-S switches currently does not support multiple VDCs. All device resources are managed in the default VDC.



CHAPTER 3

Using Modular QoS CLI

This chapter contains the following sections:

About MQC

Cisco Modular Quality of Service Command Line Interface (MQC) provides a language to define QoS policies.

You configure QoS policies by following these three steps:

1. Define traffic classes.
2. Associate policies and actions with each traffic class.
3. Attach policies to logical or physical interfaces.

MQC provides a command type to define traffic classes and policies:

- **policy-map**—Defines a policy map that represents a set of policies to be applied on a class-by-class basis to class maps.

  The policy map defines a set of actions to take on the associated traffic class, such as limiting the bandwidth or dropping packets.

You define the following class-map and policy-map object types when you create them:

- **network qos**—Defines MQC objects that you can use for system level-related actions.

- **qos**—Defines MQC objects that you can use for marking and policing.
- **queuing**—Defines MQC objects that you can use for queuing and scheduling.

Note The **qos** type is the default.

Egress QoS policies are not supported on the subinterfaces.

You can attach policies to ports, port channels, or subinterfaces by using the **service-policy** command.

You can view all or individual values for MQC objects by using the **show class-map** and **show policy-map** commands.

Caution In the interface configuration mode, the device can accept QoS and access control list (ACL) commands irrespective of the line card on which the interface host is up or down. However, you cannot enter the interface submode when the line card is down because the device does not accept any preconfiguration information.

Guidelines and Limitations for Modular QoS CLI

Modular QoS CLI has the following guidelines and limitations:

- On devices with R-Series line cards, data forwarding is not supported when configured with 4q mode policies. Instead, configure the device with 8q mode policies.

System Classes

The system QoS is a type of MQC target. You use a service policy to associate a policy map with the system qos target. A system QoS policy applies to all interfaces on the device unless a specific interface has an overriding service-policy configuration. The system QoS policies are used to define system classes, the classes of traffic across the entire device, and their attributes.

If service policies are configured at the interface level, the interface-level policy always takes precedence over the system class configuration or defaults.

When you configure QoS features, and the system requests MQC objects, you can use system-defined MQC objects for 8q mode.

Note Cisco Nexus 3400-S switches only support 8q mode.

On the Cisco Nexus 3400-S switches, a system class is uniquely identified by a qos-group value. A total of four system classes are supported. The device supports one default class which is always present on the device. Up to three additional system classes can be created by the administrator.

Default System Classes

The device provides the following system classes:

- Drop system class

By default, the software classifies all unicast and multicast Ethernet traffic into the default drop system class. This class is identified by qos-group 0.

Licensing Requirements for Using MQC Objects

The following table shows the licensing requirements for this feature:

Product	License Requirement
Cisco NX-OS	The QoS feature does not a require license. Any feature not included in a license package is bundled with the nx-os image and is provided at no extra charge to you. For a complete explanation of the Cisco NX-OS licensing scheme, see the Cisco NX-OS Licensing Guide.

Using an MQC Object

You configure QoS and queuing policies using the MQC class-map and policy-map objects. After you configure class maps and policy maps, you can attach one policy map of each type to an interface. A QoS policy can only be applied to the ingress direction.

A policy map contains either a QoS policy or queuing policy. The policy map references the names of class maps that represent traffic classes. For each class of traffic, the device applies the policies on the interface or VLAN that you select.

A packet is matched sequentially to a class of traffic starting from the first traffic class definition. When a match is found, the policy actions for that class are applied to the packet.

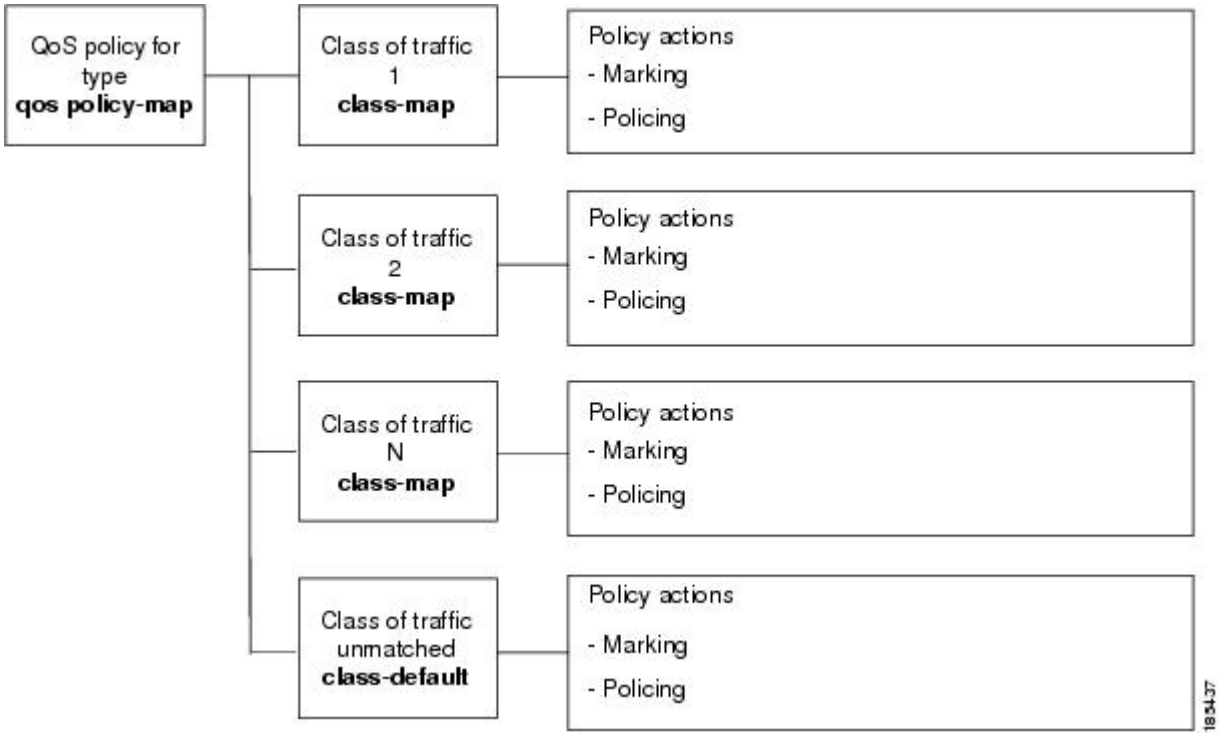
The reserved class map class-default receives all traffic that is not matched in type qos policies, and the device applies the policy actions as it would for any other traffic class.

Type qos Policies

You use type qos policies to mark and to police packets.

The following figure shows the QoS policy structure with the associated MQC objects of type qos. The MQC objects are shown in bold.

Figure 1: QoS Policy Diagram Showing Type qos MQC Object Usage

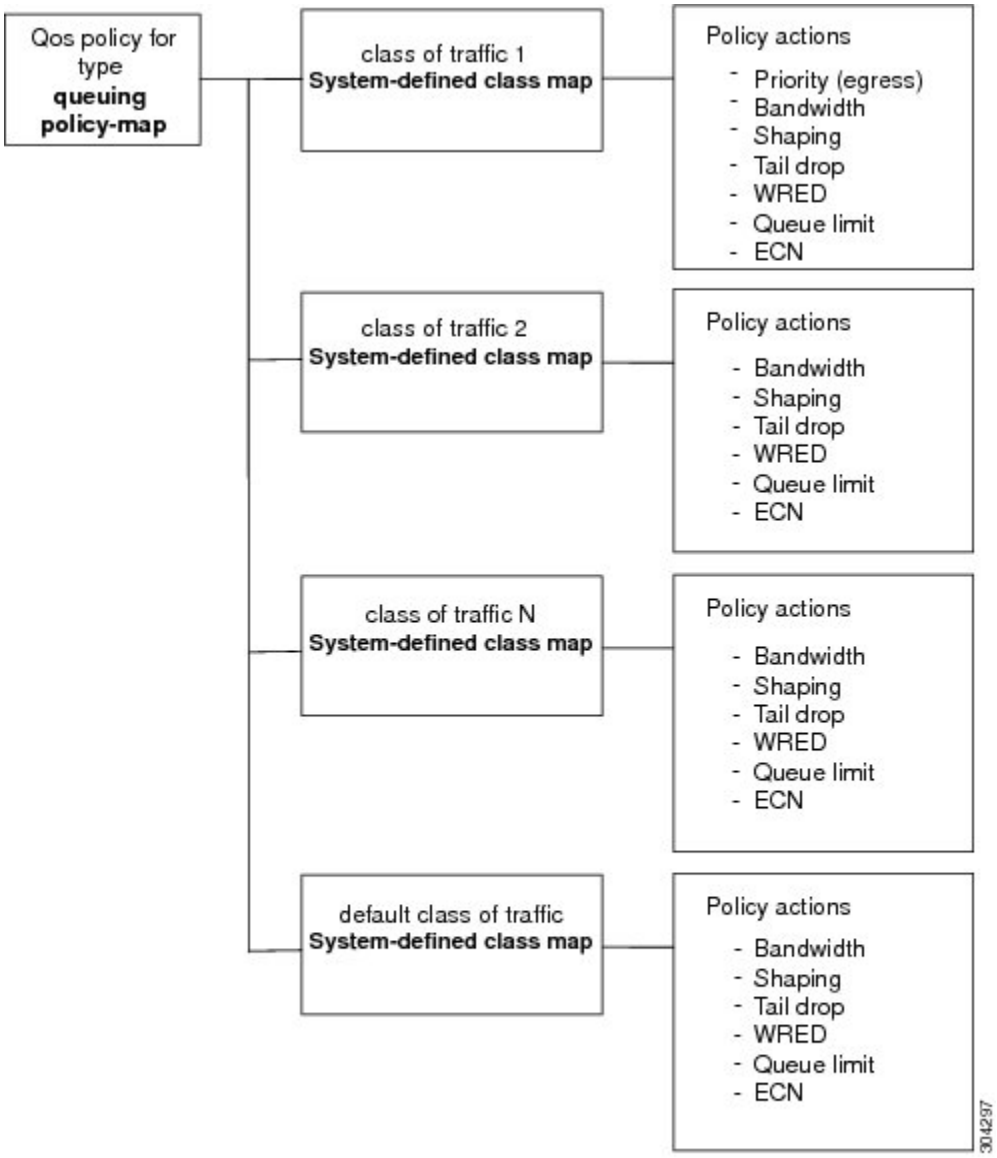


Type Queuing Policies

You use type queuing policies to shape and queue packets.

The following figure shows the QoS policy structure with associated MQC objects of type queuing. The MQC objects are shown in bold.

Figure 2: QoS Policy Diagram Showing Type Queuing MQC Object Usage



Note: See the "Configuring Queuing and Scheduling" chapter for information on configuring these parameters.

System-Defined MQC Objects

When you configure QoS features, and the system requests MQC objects, you can use system-defined objects for 8q mode.

Note Cisco Nexus 3400-S switches only support 8q mode.

System-Defined MQC Objects for 8q Mode

When you configure QoS features, and the system requests MQC objects, you can use the following system-defined objects:

Note System-defined MQC objects for 4q mode are the default MQC objects. You must enable the following MQC objects to change to 8q mode.

- Type qos class maps

Table 3: System-Defined Type qos Class Maps

Class Map Name	Description
class-default	Type qos class map that is assigned to all packets that match none of the criteria of traffic classes that you define in a type qos policy map.

- Type queuing class maps

Table 4: System-Defined Type queuing Class Maps for 8q Mode (Egress)

Class Map Queue Name	Description
c-out-8q-q-default	Egress default queue — QoS group 0
c-out-8q-q1	Egress queue 1 — QoS group 1
c-out-8q-q2	Egress queue 2 — QoS group 2
c-out-8q-q3	Egress queue 3 — QoS group 3
c-out-8q-q4	Egress queue 4 — QoS group 4
c-out-8q-q5	Egress queue 5 — QoS group 5
c-out-8q-q6	Egress queue 6 — QoS group 6
c-out-8q-q7	Egress queue 7 — QoS group 7

Table 5: System-Defined Type queuing Class Maps for 8q Mode (Ingress)

Class Map Queue Name	Description
c-in-q-default	Ingress default queue — QoS group 0
c-in-q1	Ingress queue 1 — QoS group 1
c-in-q2	Ingress queue 2 — QoS group 2
c-in-q3	Ingress queue 3 — QoS group 3
c-in-q4	Ingress queue 4 — QoS group 4

Class Map Queue Name	Description
c-in-q5	Ingress queue 5 — QoS group 5
c-in-q6	Ingress queue 6 — QoS group 6
c-in-q7	Ingress queue 7 — QoS group 7

- Type network-qos class maps

Table 6: System-Defined Type network-qos Class Maps for 8q Mode

Class Map Network-QoS Name	Description
c-8q-nq-default	Network-qos class — QoS group 0
c-8q-nq1	Network-qos class — QoS group 1
c-8q-nq2	Network-qos class — QoS group 2
c-8q-nq3	Network-qos class — QoS group 3
c-8q-nq4	Network-qos class — QoS group 4
c-8q-nq5	Network-qos class — QoS group 5
c-8q-nq6	Network-qos class — QoS group 6
c-8q-nq7	Network-qos class — QoS group 7

- Policy maps

Table 7: System-Defined Queuing Policy Maps for 8q Mode

Queuing Policy Map Name	Description
default-8q-out-policy	Output queuing policy map that is attached to all module ports to which you do not apply a queuing policy map. The default configuration values are as follows: `policy-map type queuing default-8q-out-policy` `  class type queuing c-out-8q-q7` `   priority level 1` `  class type queuing c-out-8q-q6` `   bandwidth remaining percent 0` `  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 0` `  class type queuing c-out-8q-q2` `   bandwidth remaining percent 0` `  class type queuing c-out-8q-q1` `   bandwidth remaining percent 0` `  class type queuing c-out-8q-q-default` `   bandwidth remaining percent 100`
default-8q-network-qos-policy	Network-qos queuing policy map that is attached to all module ports to which you do not apply a queuing policy map. The default configuration values are as follows: `policy-map type network-qos default-8q-nq-policy` `  class type network-qos c-8q-nq7` `   match qos-group 7` `   mtu 1500` `  class type network-qos c-8q-nq6` `   match qos-group 6` `   mtu 1500` `  class type network-qos c-8q-nq5` `   match qos-group 5` `   mtu 1500` `  class type network-qos c-8q-nq4` `   match qos-group 4` `   mtu 1500` `  class type network-qos c-8q-nq3` `   match qos-group 3` `   mtu 1500` `  class type network-qos c-8q-nq2` `   match qos-group 2` `   mtu 1500` `  class type network-qos c-8q-nq1` `   match qos-group 1` `   mtu 1500` `  class type network-qos c-8q-nq-default` `   match qos-group 0` `   mtu 1500`

Changing to 8q Mode

Note The Cisco NX-OS software operates in 8q mode by default.

Use the following guidelines to change to 8q mode:

- Change the network-qos policy to 8q mode.

  You can either activate the default-8q-nq-policy (which is the system created 8q default network-qos policy); or you can copy it using the **qos copy policy-map type network-qos** command, edit it as needed, and activate it.

- Change the queuing policy to 8q mode. (This means changing the system queuing policy and optionally any interface queuing policy.)

  Make a copy of the default-8q-out-policy (the default 8q queuing policy created by the system) using the **qos copy policy-map type queuing** command. Edit the copy of the default-8q-out-policy as needed and activate it at the system level and optionally at the interface level.

- After the network-qos and queuing policies are changed to 8q mode, you can start using **set qos-group** action for qos-groups 4-7 to steer the traffic to queues 4-7.

Example of set qos-groups

The following is an example to set qos-groups with values 4-7.

```
switch(config)# policy-map p1
switch(config-pmap-qos)# class c1
switch(config-pmap-c-qos)# set qos-group 1
switch(config-pmap-c-qos)# ex
switch(config-pmap-qos)# class c2
switch(config-pmap-c-qos)# set qos-group 4
switch(config-pmap-c-qos)# ex
switch(config-pmap-qos)# class c3
switch(config-pmap-c-qos)# set qos-group 7
switch(config-pmap-c-qos)# ex
switch(config-pmap-qos)# ex
switch(config)# show policy-map p1


  Type qos policy-maps
  ====================

  policy-map type qos p1
    class  c1
      set qos-group 1
    class  c2
      set qos-group 4
    class  c3
      set qos-group 7
switch(config)# conf t
switch(config)# int ethernet 2/1
switch(config-if)# service-policy type qos input p1
switch(config-if)# show policy-map interface ethernet 2/1


Global statistics status :   enabled
```

```
Ethernet2/1

  Service-policy (qos) input:   p1
    SNMP Policy Index:  285226505

    Class-map (qos):   c1 (match-all)
      Match: dscp 10
      set qos-group 1

    Class-map (qos):   c2 (match-all)
      Match: dscp 20
      set qos-group 4

    Class-map (qos):   c3 (match-all)
      Match: dscp 30
      set qos-group 7
```

Configuring an MQC Object

When you specify an MQC object command, the device creates the object if it does not exist and then enters map mode.

To remove a class-map or policy-map object, use the **no** form of the command that you used to create the object.

Configuring or Modifying a Class Map

You can create or modify a class map. You can then reference class maps in policy maps.

Note You cannot create a queuing class map; you must use one of the system-defined queuing class maps.

SUMMARY STEPS

1. **configure terminal**
2. **class-map type qos** [**match-any** | **match-all**] *class-name*
3. **exit**
4. **class-map type queuing match-any** *class-name*
5. **exit**
6. **show class-map** [**type qos** [*class-name*]]
7. **show class-map** [**type queuing** [*class-name*]]
8. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `switch# configure terminal` `switch(config)#`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**class-map type qos** [**match-any** | **match-all**] *class-name* **Example:** `switch(config)# class-map type qos class1` `switch(config-cmap-qos)#`	Creates or accesses the class map of type qos and then enters class-map qos mode. Class-map names can contain alphabetic, hyphen, or underscore characters, are case sensitive, and can be up to 40 characters.
Step 3	**exit** **Example:** `switch(config-cmap-qos)# exit` `switch(config)#`	Exits class-map qos mode and enters global configuration mode.
Step 4	**class-map type queuing match-any** *class-name* **Example:** `switch(config)# class-map type queuing match-any c-out-q2` `switch(config-cmap-que)#`	Creates or accesses the class map of type queuing and then enters class-map queuing mode.
Step 5	**exit** **Example:** `switch(config-cmap-que)# exit` `switch(config)#`	Exits class map queuing mode and enters global configuration mode.
Step 6	**show class-map** [**type qos** [*class-name*]] **Example:** `switch(config)# show class-map type qos`	(Optional) Displays information about all configured class maps, all class maps of type qos, or a selected class map of type qos.
Step 7	**show class-map** [**type queuing** [*class-name*]] **Example:** `switch(config)# show class-map type queuing`	(Optional) Displays information about all configured class maps, all class maps of type queuing, or a selected class map of type queuing.
Step 8	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	(Optional) Saves the running configuration to the startup configuration.

Configuring or Modifying a Policy Map

You can create or modify a policy map that you can use to define actions to perform on class maps.

SUMMARY STEPS

1. **configure terminal**
2. **policy-map type qos** { [**match-first**] *policy-map-name*}
3. **exit**
4. **policy-map type queuing** {[**match-first**] *policy-map-name}*
5. **exit**
6. **show policy-map** [**type qos** [*policy-map-name*]]
7. **show policy-map** [**type queuing** [*policy-map-name* | *default-out-policy*]]

8. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `switch# configure terminal` `switch(config)#`	Enters global configuration mode.
Step 2	**policy-map type qos** { [**match-first**] *policy-map-name*} **Example:** `switch(config)# policy-map type qos policy1` `switch(config-pmap-qos)#`	Creates or accesses the policy map of type qos and then enters policy-map mode. Policy-map names can contain alphabetic, hyphen, or underscore characters, are case sensitive, and can be up to 40 characters.
Step 3	**exit** **Example:** `switch(config-pmap)# exit` `switch(config)#`	Exits policy-map mode and enters global configuration mode.
Step 4	**policy-map type queuing** {[**match-first**] *policy-map-name}* **Example:** `switch(config)# policy-map type queuing policy_queue1` `switch(config-pmap-que)#`	Configures the policy map of type queuing and then enters policy-map mode for the policy-map name you specify. Policy-map names can contain alphabetic, hyphen, or underscore characters, are case sensitive, and can be up to 40 characters.
Step 5	**exit** **Example:** `switch(config-pmap)# exit` `switch(config)#`	Exits policy map mode and enters global configuration mode.
Step 6	**show policy-map** [**type qos** [*policy-map-name*]] **Example:** `switch(config)# show policy-map type qos`	(Optional) Displays information about all configured policy maps, all policy maps of type qos, or a selected policy map of type qos.
Step 7	**show policy-map** [**type queuing** [*policy-map-name* | *default-out-policy*]] **Example:** `switch(config)# show policy-map type queuing`	(Optional) Displays information about all configured policy maps, all policy maps of type queuing, a selected policy map of type queuing or the default output queuing policy.
Step 8	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	(Optional) Saves the running configuration to the startup configuration.

Applying Descriptions to MQC Objects

You can use the **description** command to add a description to a MQC object.

SUMMARY STEPS

1. **configure terminal**
2. Specify the MQC object whose description you want to set:
   - Class-map:

     class-map [**type qos**] [**match-any** | **match-all**] *class-name*
   - Policy-map:

     policy-map [**type qos**] [**match-first**] *policy-map-name*
3. **description** *string*
4. **exit**
5. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `switch# configure terminal` `switch(config)#`	Enters global configuration mode.
Step 2	Specify the MQC object whose description you want to set: • Class-map: **class-map** [**type qos**] [**match-any** | **match-all**] *class-name* • Policy-map: **policy-map** [**type qos**] [**match-first**] *policy-map-name* **Example:** • Class-map: `switch(config-cmap)# class-map class1` `switch(config-cmap)#` • Policy-map: `switch(config)# policy-map policy1` `switch(config-pmap)#`	• Class-map: Creates or accesses the class map and then enters class-map mode. The class-map name can contain alphabetic, hyphen, or underscore characters, is case sensitive, and can be up to 40 alphanumeric characters. • Policy-map: Creates or accesses the policy map and then enters policy-map mode. The policy-map name can contain alphabetic, hyphen, or underscore characters, is case sensitive, and can be up to 40 characters.
Step 3	**description** *string* **Example:** `switch(config-cmap)# description my traffic class` `switch(config-cmap)#`	Adds a description string to the MQC object. The description can be up to 200 alphanumeric characters. **Note** You cannot modify the description of system-defined queuing class maps.
Step 4	**exit** **Example:** `switch(config-cmap)# exit` `switch(config)#`	Exits class-map mode and enters global configuration mode.

	Command or Action	Purpose
Step 5	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	(Optional) Saves the running configuration to the startup configuration.

Verifying an MQC Object

To display MQC object configuration information, perform one of the following tasks:

Command	Purpose
show class-map [**type qos** [*class-name*]]	Displays information about all configured class maps, all class maps of type qos, or a selected class map of type qos.
show class-map [**type queuing** [*class-name*]]	Displays information about all configured class maps, all class maps of type queuing, or a selected class map of type queuing.
show policy-map [**type qos** [*policy-map-name*]]	Displays information about all configured policy maps, all policy maps of type qos, or a selected policy map of type qos.
show policy-map [**type queuing** [*policy-map-name* | **default-out-policy**]]	Displays information about all configured policy maps, all policy maps of type queuing, a selected policy map of type queuing, or the default output queuing policy.

Attaching and Detaching a QoS Policy Action

The software does not allow you to enable or disable QoS features with a configuration command. To enable or disable QoS features, you must attach or detach QoS policies to or from interfaces or VLANs as described in this section.

The system-defined type queuing policy maps are attached to each interface unless you specifically attach a different policy map.

Note The device allows only one queuing policy per interface.

Policies that are defined at multiple interfaces have the following restrictions:

- A QoS policy attached to the physical port takes effect when the port is not a member of a port channel.
- A QoS policy attached to a port channel takes effect even when policies are attached to member ports.
- A QoS policy attached to a VLAN is applied to all ports in that VLAN that do not have other policies specifically applied.
- One ingress QoS policy is supported for each Layer 3 port and Layer 3 port-channel interface.
- One ingress QoS policy is supported for each VLAN.

- When a VLAN or port channel, or both, touches multiple forwarding engines, all policies that enforce a rate are enforced per forwarding engine.

  For example, if you configure a policer on a specific VLAN that limits the rate for the VLAN to 100 Mbps and if you configure one switch port in the VLAN on one module and another switch port in the VLAN on another module, each forwarding engine can enforce the 100-Mbps rate. In this case, you could actually have up to 200 Mbps in the VLAN that you configured to limit the rate to 100 Mbps.

Note Default queuing policies are active, unless you configure and apply another policy.

The interface where a QoS policy is applied is summarized in the following table. Each row represents the interface levels. The entry descriptions are as follows:

- Applied—Interface where an attached policy is applied.
- Present—Interface where a policy is attached but not applied.
- Not present—Interface where no policy is attached.
- Present or not—Interface where a policy is either attached or not, but not applied.

Table 8: QoS Policy Interfaces

Port Policy	Port-Channel Policy	VLAN Policy
Applied	Not present	Present or not
Present or not	Applied	Present or not
Not present	Not present	Applied

To attach a policy map to an interface or VLAN, use the **service-policy** command. The policies defined in the policy map are applied to the input stream of packets on the interface.

To detach a policy map from an interface, use the **no** form of the **service-policy** command.

Configuring a Service Policy for a Layer 2 Interface

Before you begin

Ensure that the ternary content addressable memory (TCAM) is carved for port QoS.

For more details, see the Configuring QoS TCAM Carving section.

SUMMARY STEPS

1. **configure terminal**
2. **interface interface** *slot/port*
3. **switchport**

4. **service-policy type** {**qos input** | **queuing output**} | {**qos output** | **queuing output**} *policy-map-name* [**no-stats**]
5. **show policy-map interface** *interface slot/port* **type** {**qos** | **queuing**}
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `switch# configure terminal` `switch(config)#`	Enters global configuration mode.
Step 2	**interface interface** *slot/port* **Example:** `switch(config)# interface ethernet 1/1` `switch(config-if)#`	Enters configuration interface mode.
Step 3	**switchport** **Example:** `switch(config-if)# switchport`	Selects the Layer 2 interface.
Step 4	**service-policy type** {**qos input**	**queuing output**}	{**qos output**	**queuing output**} *policy-map-name* [**no-stats**] **Example:** `switch(config-if)# service-policy input policy1` `switch(config-if)#` **Example:** `switch(config-if)# interface intf1` `switch(config-if)# service-policy type qos output egressqos` `switch(config-if)# exit` `switch(config)#`	Specifies the policy map to use as the service policy for the Layer 2 interface. There are two policy-map configuration modes: • qos input or qos output — qos input is the default classification mode. To set the classification mode to egress, use qos output. • queuing output —Queuing mode. **Note** The **output** keyword specifies that this policy map should be applied to traffic transmitted from an interface. You can only apply **output** to a queuing policy.
Step 5	**show policy-map interface** *interface slot/port* **type** {**qos**	**queuing**} **Example:** `switch(config)# show policy-map interface ethernet 1/1 type qos`	(Optional) Displays information about policy maps that are applied to the specified interface. You can limit what the device displays to qos or queuing policies.
Step 6	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	(Optional) Saves the running configuration to the startup configuration.

Configuring a Service Policy for a Layer 3 Interface

Before you begin

Ensure that the ternary content addressable memory (TCAM) is carved for Layer 3 QoS.

For more details, see the Configuring QoS TCAM Carving section.

SUMMARY STEPS

1. **configure terminal**
2. **interface interface** *slot/port*
3. **no switchport**
4. **service-policy type** {**qos input** | **queuing output**} | {**qos output** | **queuing output**} *policy-map-name* [**no-stats**]
5. **show policy-map interface** *interface slot/port* **type** {**qos** | **queuing**}
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `switch# configure terminal` `switch(config)#`	Enters global configuration mode.
Step 2	**interface interface** *slot/port* **Example:** `switch(config)# interface ethernet 1/1` `switch(config-if)#`	Enters configuration interface mode.
Step 3	**no switchport** **Example:** `switch(config-if)# no switchport`	Selects the Layer 3 interface.
Step 4	**service-policy type** {**qos input**	**queuing output**}	{**qos output**	**queuing output**} *policy-map-name* [**no-stats**] **Example:** `switch(config-if)# service-policy input policy1` `switch(config-if)#` **Example:** `switch(config-if)# service-policy output policy1` `switch(config-if)#`	Specifies the policy map to use as the service policy for the Layer 3 interface. There are two policy-map configuration modes: • qos input or qos output — qos input is the default classification mode. To set the classification mode to egress, use qos output. • queuing output —Queuing mode. **Note** The **output** keyword specifies that this policy map should be applied to traffic transmitted from an interface. You can only apply **output** to a queuing policy.

	Command or Action	Purpose
Step 5	**show policy-map interface** *interface slot/port* **type** {**qos** | **queuing**} **Example:** `switch(config)# show policy-map interface ethernet 1/1 type qos`	(Optional) Displays information about policy maps that are applied to the specified interface. You can limit what the device displays to qos or queuing policies.
Step 6	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	(Optional) Saves the running configuration to the startup configuration.

Attaching the System Service Policy

The **service-policy** command specifies the system class policy map as the service policy for the system.

SUMMARY STEPS

1. **configure terminal**
2. **system qos**
3. **service-policy type** {**network-qos** | **queuing output**} *policy-map-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `switch# configure terminal` `switch(config)#`	Enters global configuration mode.
Step 2	**system qos** **Example:** `switch(config)# system qos` `switch(config-sys-qos)#`	Enters system class configuration mode.
Step 3	**service-policy type** {**network-qos** | **queuing output**} *policy-map-name* **Example:** `switch(config-sys-qos)# service-policy input default-nq-policy`	Specifies the policy map to use as the service policy (default-nq-policy) for the system. There are two policy-map configuration modes: • network-qos—Network-wide (system qos) mode. **Note** To restore the system to the default service policies, use the **no** form of the command. • queuing—Queuing mode (output at system qos and interface).

	Command or Action	Purpose
		Note There is no default policy-map configuration mode. You must specify the type. The **output** keyword specifies that this policy map should be applied to traffic transmitted from an interface. You can only apply **output** to a queuing policy.

Attaching a QoS Policy Action to a VLAN

Before you begin

Ensure that the ternary content-addressable memory (TCAM) is carved for VLAN QoS.

For more details, see the QoS TCAM carving chapter.

Note Cisco Nexus 3400-S switches do not support VLAN-based classification.

SUMMARY STEPS

1. **configure terminal**
2. **vlan configuration** *vlan-id-list*
3. **service-policy** [**type qos**] {**input**} | {**qos output** } {*policy-map-name*} [**no-stats**]
4. **show policy-map** [**interface** *interface* | **vlan** *vlan-id*] [**input**] [**type qos** | **queuing**] [**class** [**type qos** | **queuing**] *class-map-name*]
5. **copy running-config startup-config**

DETAILED STEPS

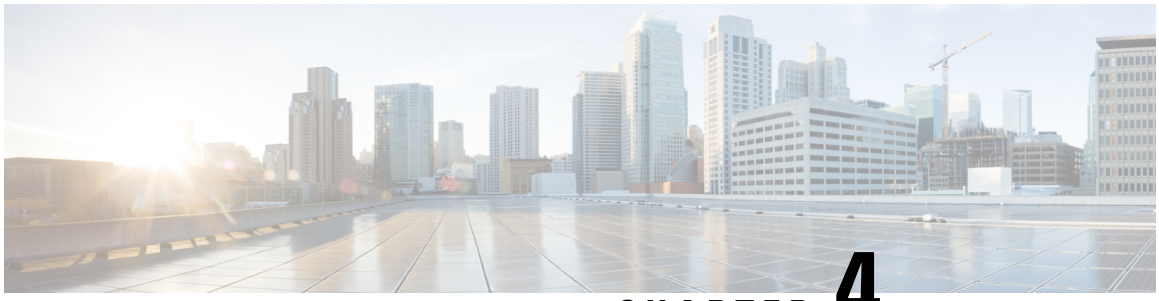
	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `switch# configure terminal` `switch(config)#`	Enters global configuration mode.
Step 2	**vlan configuration** *vlan-id-list* **Example:** `switch(config)# vlan configuration 2` `switch(config-vlan-config)#`	Enters VLAN configuration mode. **Note** *vlan-id-list* is a space-separated list of VLANs.
Step 3	**service-policy** [**type qos**] {**input**} | {**qos output** } {*policy-map-name*} [**no-stats**] **Example:**	Adds the policy map to the input packets of a VLAN. Only one input policy can be attached to a VLAN. The example adds policy1 to the VLAN.

	Command or Action	Purpose
	`switch(config-vlan-config)# service-policy type qos input policy1` **Example:** `switch(config-if)# service-policy type qos output egressqos` `switch(config-if)# exit` `switch(config)#`	Label sharing only occurs when QoS policies under VLANs are configured with the **no-stats** option. With the **no-stats** option, the QoS label gets shared when the same QoS policy is applied on multiple VLANs. **Note** When the **no-stats** option is configured, the ingress QoS policy-map statistics on a VLAN basis are not available because the label is shared.
Step 4	**show policy-map** [**interface** *interface* | **vlan** *vlan-id*] [**input**] [**type qos** | **queuing**] [**class** [**type qos** | **queuing**] *class-map-name*] **Example:** `switch(config)# show policy-map vlan 2`	(Optional) Displays information about policy maps that are applied to all interfaces or the specified interface. You can limit what the device displays to input policies, qos or queuing polices, and to a specific class.
Step 5	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	(Optional) Saves the running configuration to the startup configuration.

Session Manager Support for QoS

Session Manger supports the configuration of QoS. This feature allows you to verify the QoS configuration and confirm that the resources required by the configuration are available prior to committing them to the running configuration. For information about Session Manager, see the *Cisco Nexus 3400-S Series NX-OS System Management Configuration Guide*.

After you start the configuration session, do not enter any configuration commands using the configure terminal configuration mode until the configuration session is aborted or committed. Entering parallel configurations (one configuration that uses the configuration session and another using the configuration terminal configuration mode) might cause verification failures in the configuration session mode.



CHAPTER 4

Configuring QoS TCAM Carving

This chapter contains the following sections:

About QoS TCAM Carving

You can change the size of the access control list (ACL) ternary content addressable memory (TCAM) regions in the hardware. Both ingress and egress TCAM regions can be altered.

Ingress TCAM Region Features

Ingress TCAM regions are comprised of the following layout and sizes:

- Total TCAM size: 3.5K, 80 bit wide
- Total Counters: 3.5K
- Configurable width: 80 bit, 160 bit, 320 bit
- Configurable depth: 128, 256 or multiples of 256
- Max lookup: 10

For ingress TCAM, there are three logical QoS regions:

- `ing-l2-qos`
- `ing-l3-vlan-qos`
- `ing-l2-l3-qos`

For carving the above three regions, the following limitations apply:

- If you carve `ing-l2-l3-qos`, then `ing-l2-qos` or `ing-l3-vlan-qos` cannot be carved.
- If you carve `ing-l2-qos` and `ing-l3-vlan-qos`, each of these two logical regions matches to a separate physical TCAM region.

Table 9: Ingress TCAM Specifications

Feature	Width	Lookup	Default Carving
PACL MAC	160 bit	1	No
PACL IPv4	160 bit	1	No
PACL IPv6	320 bit	2	No
RACL IPv4	160 bit	1	Yes (size: 256)
RACL IPv4 UDF	320 bit	2	No
RACL IPv6	320 bit	2	No
VACL MAC	160 bit	1	No
VACL IPv4	160 bit	1	No
VACL IPv6	320 bit	2	No
L2 QoS	320 bit	2	No
L3-VLAN QoS	320 bit	2	Yes (size: 128)
L2-L3 QoS	320	2	No
SPAN	160 bit	1	Yes (size: 128)
SUP	320 bit	2	No
VPC Convergence	80 bit	1	No
Storm Control	80	1	Yes (size: 256)

Egress TCAM Region Features

Egress TCAM regions are comprised of the following layout and sizes:

- Total TCAM size: 1.5K, 80 bit wide
- Total Counters: 1.5K
- Configurable width: 80 bit, 160 bit, 320 bit
- Configurable depth: 128, 256 or multiples of 256
- Max lookup: 4

Table 10: Egress TCAM Specifications

Feature	Width	Lookup	Default Carving
RACL IPv4	160 bit	1	No
RACL IPv6	320 bit	2	No

Feature	Width	Lookup	Default Carving
VACL MAC	160 bit	1	No
VACL IPv4	160 bit	1	No
VACL IPv6	320 bit	2	No
L2 QoS	160 bit	2	No
L3 VLAN QoS	160 bit	2	No
PFC Counter	80 bit	1	Yes (size: 256)

You must save the configuration and reload the system for the region configuration to become effective.

Guidelines and Limitations for QoS TCAM Carving

Note For scale information, see the release-specific *Cisco Nexus 3400-S NX-OS Verified Scalability Guide*.

TCAM carving has the following guidelines and limitations:

- Egress QoS features are not supported. Therefore, egress QoS TCAM carving is blocked.
- **show** commands with the **internal** keyword are not supported.
- After TCAM carving, you must save the configuration and reload the switch.
- Use the **show hardware access-list tcam region** command to view the configured TCAM region size.
- TCAM templates are not supported.

Configuring QoS TCAM Carving

You can change the default QoS TCAM carving to accommodate your network requirements. The following sections contain examples of how to change the default QoS TCAM carving.

SUMMARY STEPS

1. **show hardware access-list tcam region**
2. **hardware access-list tcam region** {**e-ipv6-racl** | **e-racl** | **eor-l2-qos** | **egr-l3-vlan** | **ifacl** | **ing-l2-qos** | **ing-l3-vlan-qos** | **ing-sup** | **ipv6-ifacl** |**ipv6-racl** |**ipv6-vacl** | **mac-ifacl** |**mac-vacl racl** |**span** |**vacl** |**vpc-convergence** } *tcam-size*
3. **hardware access-list tcam region** {**e-ipv6-racl** | **e-racl** | **eor-l2-qos** | **egr-l3-vlan** | **ifacl** | **ing-l2-qos** | **ing-l3-vlan-qos** | **ing-sup** | **ipv6-ifacl** |**ipv6-racl** |**ipv6-vacl** | **mac-ifacl** |**mac-vacl racl** |**span** |**vacl** |**vpc-convergence** } *tcam-size*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**show hardware access-list tcam region** **Example:** `switch# show hardware access-list tcam region` `IPV4 PACL [ifacl]` `size = 0` `IPV6 PACL [ipv6-ifacl]` `size = 0` `MAC PACL [mac-ifacl]` `size = 0` `IPV4 VACL [vacl]` `size = 0` `IPV6 VACL [ipv6-vacl]` `size = 0` `MAC VACL [mac-vacl]` `size = 0` `IPV4 RACL [racl]` `size = 256` `IPV6 RACL [ipv6-racl]` `size = 0` `Egress IPV4 RACL [e-racl]` `size = 0` `Egress IPV6 RACL [e-ipv6-racl]` `size = 0` `SPAN [span]` `size = 0` `VPC Convergence/ES-Multi Home [vpc-convergence]` `size = 0` `Ingress L2 QOS [ing-l2-qos]` `size = 0` `Ingress L3/VLAN QOS [ing-l3-vlan-qos]` `size = 128` `Ingress SUP [ing-sup]` `size = 256` `Egress L2 QOS [egr-l2-qos]` `size = 0` `Egress L3/VLAN QOS [egr-l3-vlan-qos]` `size = 0`	View the current size of all TCAM regions. This shows the regions you can reduce so you can increase another region.
Step 2	**hardware access-list tcam region** {**e-ipv6-racl** | **e-racl** | **eor-l2-qos** | **egr-l3-vlan** | **ifacl** | **ing-l2-qos** | **ing-l3-vlan-qos** | **ing-sup** | **ipv6-ifacl** |**ipv6-racl** |**ipv6-vacl** | **mac-ifacl** |**mac-vacl racl** |**span** |**vacl** |**vpc-convergence** } *tcam-size* **Example:** `switch(config)# hardware access-list tcam region ipv6-racl 128` `Warning: Please save config and reload the system for the configuration to take effect` `switch(config)#`	To enable carving of another TCAM region, specify a region to free up resources. Also specify the reduced TCAM size for the region.
Step 3	**hardware access-list tcam region** {**e-ipv6-racl** | **e-racl** | **eor-l2-qos** | **egr-l3-vlan** | **ifacl** | **ing-l2-qos** | **ing-l3-vlan-qos** | **ing-sup** | **ipv6-ifacl** |**ipv6-racl** |**ipv6-vacl** | **mac-ifacl** |**mac-vacl racl** |**span** |**vacl** |**vpc-convergence** } *tcam-size* **Example:**	To carve a TCAM region, specify the region and the TCAM size (the size you freed up in the previous step) for the region.

	Command or Action	Purpose
	`switch(config)# hardware access-list tcam region vacl 128` `Warning: Please save config and reload the system for the configuration to take effect` `switch(config)#`	

Verifying QoS TCAM Carving

After you adjust the TCAM region sizes, enter the **show hardware access-list tcam region** command to display the TCAM sizes that will be applicable on the next reload of the device.

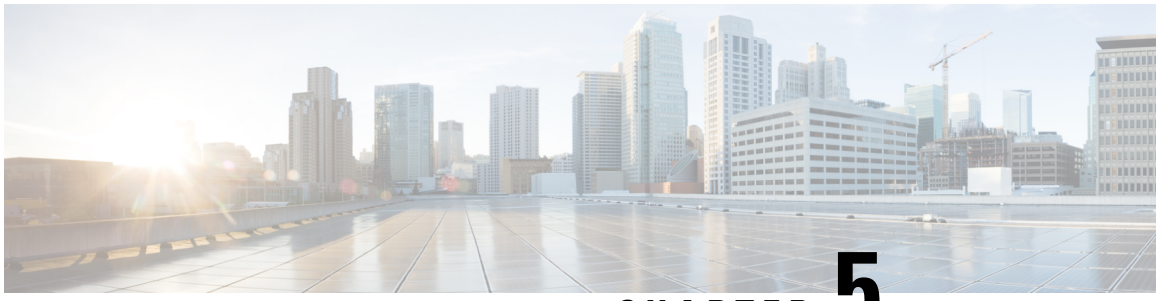
Note To keep all modules synchronized, you must reload all line card modules or enter the **copy running-config startup-config** command and the **reload** command to reload the device. Multiple TCAM region configurations require only a single reload. You can wait until you complete all of your TCAM region configurations before you reload the device.

If you exceed the 4K ingress limit for all TCAM regions when you configure a TCAM region, the following message appears:

```
ERROR: Aggregate TCAM region configuration exceeded the available Ingress TCAM space.
Please re-configure.
```

If TCAM for a particular feature is not configured and you try to apply a feature that requires TCAM carving, the following message appears:

```
ERROR: Module x returned status: TCAM region is not configured. Please configure TCAM
region and retry the command.
```



CHAPTER 5

Configuring Classification

This chapter contains the following sections:

About Classification

Classification is the separation of packets into traffic classes. You configure the device to take a specific action on the specified classified traffic, such as policing or marking down, or other actions.

You can create class maps to represent each traffic class by matching packet characteristics with the classification criteria in the following table:

Table 11: Classification Criteria

Classification Criteria	Description
CoS	Class of service (CoS) field in the IEEE 802.1Q header.
IP precedence	Precedence value within the type of service (ToS) byte of the IP header.
Differentiated Services Code Point (DSCP)	DSCP value within the DiffServ field of the IP header.
ACL	IP, IPv6, or MAC ACL name.
Packet length	Size range of Layer 3 packet lengths.
IP RTP	Identify applications using Real-time Transport Protocol (RTP) by UDP port number range.

You can specify multiple match criteria, you can choose to not match on a particular criterion, or you can determine the traffic class by matching any or all criteria.

Note However, if you match on an ACL, no other match criteria, except the packet length, can be specified in a match-all class. In a match-any class, you can match on ACLs and any other match criteria.

Traffic that fails to match any class in a QoS policy map is assigned to a default class of traffic called class-default. The class-default can be referenced in a QoS policy map to select this unmatched traffic.

You can reuse class maps when defining the QoS policies for different interfaces that process the same types of traffic.

Licensing Requirements for Classification

The following table shows the licensing requirements for this feature:

Product	License Requirement
Cisco NX-OS	The QoS feature does not require a license. Any feature not included in a license package is bundled with the NX-OS image and is provided at no extra charge to you. For a complete explanation of the Cisco NX-OS licensing scheme, see the Cisco NX-OS Licensing Guide.

Prerequisites for Classification

Classification has the following prerequisites:

- You must be familiar with using modular QoS CLI.
- You are logged on to the device.

Guidelines and Limitations for Classification

Classification has the following guidelines and limitations:

- A QoS policy that references an ACL that contains a match on a source IPv6 address is not supported. Only matching on IPv4 source/destination and IPv6 destination in supported.
- A match on CoS/DSCP creates entries for IPv4/IPv6 which requires double the TCAM entries.
- Port-range matches are LOU expanded on ingress only.
- MAC address based match is not supported.
- RTP list not supported as match criteria in **class-map** for QoS classification.

- You cannot set both CoS and DSCP values for a class in a policy map.
- The **show** commands with the **internal** keyword are not supported.
- Matching the packets that are based on DSCP, CoS, or precedence in Cisco Nexus 3400-S switches, the TCAM entries for both IPv4 (single-wide is one entry) and IPv6 (double-wide are two entries) are installed in the hardware. For example, if you match DSCP 4, three entries are installed in the hardware, one entry for IPv4 and two entries for IPv6.
- You can specify a maximum of 512 match criteria in a class map.
- You can configure a maximum of 128 classes for use in a single policy map.
- Packet length classification is not supported.
- The **match-all** option in the **class-map type qos match-all** command is not supported. The match criteria of this command becomes the same as in the **class-map type qos match-any** command. The **class-map type qos match-all** command yields the same results as the **class-map type qos match-any** command.
- Classification on VLANs is not supported.
- RTP classification is not supported.
- QoS classification policies are not supported under system QoS for Layer 2 switch ports. However, you can configure a QoS policy to classify the incoming traffic that is based on CoS/DSCP and map it to different queues. The QoS policy must be applied under all the interfaces that require the classification.
- MAC-based ACLs are not supported.

Configuring Traffic Classes

Configuring ACL Classification

You can classify traffic by matching packets based on an existing access control list (ACL). Traffic is classified by the criteria defined in the ACL. The permit and deny ACL keywords are ignored in the matching; even though a match criteria in the access-list has a deny action, it is still used for matching for this class.

Note Use the **class-map class_acl** command to display the ACL class-map configuration.

SUMMARY STEPS

1. **configure terminal**
2. **class-map** [**type qos**] [**match-any** | **match-all**] *class-name*
3. **match access-group name** *acl-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `switch# configure terminal` `switch(config)#`	Enters global configuration mode.
Step 2	**class-map** [**type qos**] [**match-any** | **match-all**] *class-name* **Example:** `switch(config)# class-map class_acl`	Creates or accesses the class map named class-name and enters class-map mode. The class map name can contain alphabetic, hyphen, or underscore characters, and can be up to 40 characters. (**match-any** is the default when no option is selected and multiple match statements are entered.)
Step 3	**match access-group name** *acl-name* **Example:** `switch(config-cmap-qos)# match access-group name my_acl`	Configures the traffic class by matching packets based on the *acl-name*. The **permit** and **deny** ACL keywords are ignored in the matching.

Examples: Configuring ACL Classification

To prevent packets from being matched by the QoS class-map, you must explicitly specify the packets you want to match with permit statements. The *implicit* default deny statement at the end of the ACL will filter out the remainder. Any *explicit* deny statements configured inside the access list of a QoS class map will be ignored in the matching and treated as an explicit permit statement as shown in the examples below.

The following examples, A1, B1, and C1, all produce the same QoS matching results:

- A1

```
ip access-list extended A1
  permit ip 10.1.0.0 0.0.255.255 any
  permit ip 172.16.128.0 0.0.1.255 any
  permit ip 192.168.17.0 0.0.0.255 any
```

- B1

```
ip access-list extended B1
  permit ip 10.1.0.0 0.0.255.255 any
  deny ip 172.16.128.0 0.0.1.255 any  /* deny is interpreted as a permit */
  permit ip 192.168.17.0 0.0.0.255 any
```

- C1

```
ip access-list extended C1
  deny ip 10.1.0.0 0.0.255.255 any   /* deny is interpreted as a permit */
 deny ip 172.16.128.0 0.0.1.255 any  /* deny is interpreted as a permit */
 deny ip 192.168.17.0 0.0.0.255 any  /* deny is interpreted as a permit */
```

Adding an explicit DENY ALL at the end of a QoS matching ACL causes the QoS ACL to permit all traffic.

The following examples, D1 and E1, produce the same QoS matching results:

• D1

```
ip access-list extended D1
  permit ip 10.1.0.0 0.0.255.255 any
  permit ip 172.16.128.0 0.0.1.255 any
  permit ip 192.168.17.0 0.0.0.255 any
 deny ip 0.0.0.0 255.255.255.255 any  /* deny is interpreted as a permit */
```

Note The last line in the example effectively becomes a PERMIT ALL statement and results in the QoS ACL to permit all packets.

• E1

```
ip access-list extended E1
    permit ip 0.0.0.0 255.255.255.255 any
```

Configuring DSCP Classification

You can classify traffic based on the DSCP value in the DiffServ field of the IP header. The standard DSCP values are listed in the following table:

Table 12: Standard DSCP Values

Value	List of DSCP Values
af11	AF11 dscp (001010)—decimal value 10
af12	AF12 dscp (001100)—decimal value 12
af13	AF13 dscp (001110)—decimal value 14
af21	AF21 dscp (010010)—decimal value 18
af22	AF22 dscp (010100)—decimal value 20
af23	AF23 dscp (010110)—decimal value 22
af31	AF31 dscp (011010)—decimal value 26
af32	AF40 dscp (011100)—decimal value 28
af33	AF33 dscp (011110)—decimal value 30
af41	AF41 dscp (100010)—decimal value 34
af42	AF42 dscp (100100)—decimal value 36
af43	AF43 dscp (100110)—decimal value 38
cs1	CS1 (precedence 1) dscp (001000)—decimal value 8
cs2	CS2 (precedence 2) dscp (010000)—decimal value 16

Value	List of DSCP Values
cs3	CS3 (precedence 3) dscp (011000)—decimal value 24
cs4	CS4 (precedence 4) dscp (100000)—decimal value 32
cs5	CS5 (precedence 5) dscp (101000)—decimal value 40
cs6	CS6 (precedence 6) dscp (110000)—decimal value 48
cs7	CS7 (precedence 7) dscp (111000)—decimal value 56
default	Default dscp (000000)—decimal value 0
ef	EF dscp (101110)—decimal value 46

SUMMARY STEPS

1. **configure terminal**
2. **class-map** [**type qos**] [**match-any** | **match-all**] *class-name*
3. **match** [**not**] **dscp** *dscp-values*
4. **exit**
5. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `switch# configure terminal` `switch(config)#`	Enters global configuration mode.
Step 2	**class-map** [**type qos**] [**match-any** | **match-all**] *class-name* **Example:** `switch(config)# class-map class_dscp`	Creates or accesses the class map named class-name and enters class-map mode. The class-map name can contain alphabetic, hyphen, or underscore characters, and can be up to 40 characters.
Step 3	**match** [**not**] **dscp** *dscp-values* **Example:** `switch(config-cmap-qos)# match dscp af21, af32`	Configures the traffic class by matching packets based on dscp-values. The standard DSCP values are shown in the following table. Use the **not** keyword to match on values that do not match the specified range.
Step 4	**exit** **Example:** `switch(config-cmap-qos)# exit` `switch(config)#`	Exits global class-map queuing mode and enters global configuration mode.
Step 5	**copy running-config startup-config** **Example:**	(Optional) Saves the running configuration to the startup configuration.

	Command or Action	Purpose
	`switch(config)# copy running-config startup-config`	

Example

This example shows how to display the DSCP class-map configuration:

```
switch# show class-map class_dscp
```

Configuring IP Precedence Classification

You can classify traffic based on the precedence value in the type of service (ToS) byte field of the IP header. The precedence values are listed in the following:

Table 13: Precedence Values

Value	List of Precedence Values
0-7	IP precedence value
critical	Critical precedence (5)
flash	Flash precedence (3)
flash-override	Flash override precedence (4)
immediate	Immediate precedence (2)
internet	Internetwork control precedence (6)
network	Network control precedence (7)
priority	Priority precedence (1)
routine	Routine precedence (0)

SUMMARY STEPS

1. **configure terminal**
2. **class-map** [**type qos**] [**match-any** | **match-all**] *class-name*
3. **match** [**not**] **precedence** *precedence-values*
4. **exit**
5. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`switch# configure terminal` `switch(config)#`	
Step 2	**class-map** [**type qos**] [**match-any** | **match-all**] *class-name* **Example:** `switch(config)# class-map class_ip_precedence`	Creates or accesses the class map named class-name and then enters class-map mode. The class-map name can contain alphabetic, hyphen, or underscore characters, and can be up to 40 characters.
Step 3	**match** [**not**] **precedence** *precedence-values* **Example:** `switch(config-cmap-qos)# match precedence 1-2, 5-7`	Configures the traffic class by matching packets based on *precedence-values*. Values are shown in the following table. Use the **not** keyword to match on values that do not match the specified range.
Step 4	**exit** **Example:** `switch(config-cmap-qos)# exit` `switch(config)#`	Exits global class-map queuing mode and enters global configuration mode.
Step 5	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	(Optional) Saves the running configuration to the startup configuration.

Example

This example shows how to display the IP precedence class-map configuration:

```
switch# show class-map class_ip_precedence
```

Configuring Protocol Classification

For Layer 3 protocol traffic, you can use the ACL classification match.

Table 14: match Command Protocol Arguments

Argument	Description
arp	Address Resolution Protocol (ARP)
bridging	Bridging
cdp	Cisco Discovery Protocol (CDP)
dhcp	Dynamic Host Configuration (DHCP)
isis	Intermediate system to intermediate system (IS-IS)

SUMMARY STEPS

1. **configure terminal**
2. **class-map** [**type qos**] [**match-any** | **match-all**] *class-name*
3. **match** [**not**] **protocol** {**arp** | **bridging** | **cdp** | **dhcp** | **isis**}
4. **exit**
5. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `switch# configure terminal` `switch(config)#`	Enters global configuration mode.
Step 2	**class-map** [**type qos**] [**match-any**	**match-all**] *class-name* **Example:** `switch(config)# class-map class_protocol`	Creates or accesses the class map named class-name and then enters class-map mode. The class-map name can contain alphabetic, hyphen, or underscore characters, and can be up to 40 characters.
Step 3	**match** [**not**] **protocol** {**arp**	**bridging**	**cdp**	**dhcp**	**isis**} **Example:** `switch(config-cmap-qos)# match protocol isis`	Configures the traffic class by matching packets based on the specified protocol. Use the **not** keyword to match on protocols that do not match the protocol specified.
Step 4	**exit** **Example:** `switch(config-cmap-qos)# exit` `switch(config)#`	Exits global class-map queuing mode and enters global configuration mode.
Step 5	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	(Optional) Saves the running configuration to the startup configuration.

Example

This example shows how to display the protocol class-map configuration:

```
switch# show class-map class_protocol
```

Configuring CoS Classification

You can classify traffic based on the class of service (CoS) in the IEEE 802.1Q header. This 3-bit field is defined in IEEE 802.1p to support QoS traffic classes. CoS is encoded in the high order 3 bits of the VLAN ID Tag field and is referred to as user_priority.

SUMMARY STEPS

1. **configure terminal**
2. **class-map** [**type qos**] [**match-any** | **match-all**] *class-name*
3. **match** [**not**] **cos** *cos-list*
4. **exit**
5. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `switch# configure terminal` `switch(config)#`	Enters global configuration mode.
Step 2	**class-map** [**type qos**] [**match-any** | **match-all**] *class-name* **Example:** `switch(config)# class-map class_cos`	Creates or accesses the class map named class-name and then enters class-map mode. The class-map name can contain alphabetic, hyphen, or underscore characters, and can be up to 40 characters.
Step 3	**match** [**not**] **cos** *cos-list* **Example:** `switch(config-cmap-qos)# match cos 4,5-6`	Configures the traffic class by matching packets based on the list of CoS values. Values can range from 0 to 7. Use the **not** keyword to match on values that do not match the specified range. **Note** When a Cisco Nexus Fabric Extender (FEX) is connected and in use, data traffic should not be marked with a CoS value of 7. CoS 7 is reserved for control traffic transiting the Fabric Extender.
Step 4	**exit** **Example:** `switch(config-cmap-qos)# exit` `switch(config)#`	Exits global class-map queuing mode and enters global configuration mode.
Step 5	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	(Optional) Saves the running configuration to the startup configuration.

Example

This example shows how to display the CoS class-map configuration:

```
switch# show class-map class_cos
```

Configuring IP RTP Classification

The IP Real-time Transport Protocol (RTP) is a transport protocol for real-time applications that transmit data such as audio or video and is defined by RFC 3550. Although RTP does not use a common TCP or UDP port, you typically configure RTP to use ports 16384 to 32767. UDP communications uses an even-numbered port and the next higher odd-numbered port is used for RTP Control Protocol (RTCP) communications.

Note The Cisco Nexus 3400-S switches do not support RTP classification.

You can configure classification based on UDP port ranges, which are likely to target applications using RTP.

SUMMARY STEPS

1. **configure terminal**
2. **class-map** [**type qos**] [**match-any** | **match-all**] *class-name*
3. **match** [**not**] **ip rtp** *udp-port-value*
4. **exit**
5. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `switch# configure terminal` `switch(config)#`	Enters global configuration mode.
Step 2	**class-map** [**type qos**] [**match-any** | **match-all**] *class-name* **Example:** `switch(config)# class-map class_rtp`	Creates or accesses the class map named class-name and then enters class-map mode. The class-map name can contain alphabetic, hyphen, or underscore characters, and can be up to 40 characters.
Step 3	**match** [**not**] **ip rtp** *udp-port-value* **Example:** `switch(config-cmap-qos)# match ip rtp 2000-2100, 4000-4100`	Configures the traffic class by matching packets based on a range of lower and upper UDP port numbers, which is likely to target applications using RTP. Values can range from 2000 to 65535. Use the **not** keyword to match on values that do not match the specified range.
Step 4	**exit** **Example:** `switch(config-cmap-qos)# exit` `switch(config)#`	Exits global class-map queuing mode and enters global configuration mode.
Step 5	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	(Optional) Saves the running configuration to the startup configuration.

Example

This example shows how to display the RTP class-map configuration:

```
switch# show class-map class_rtp
```

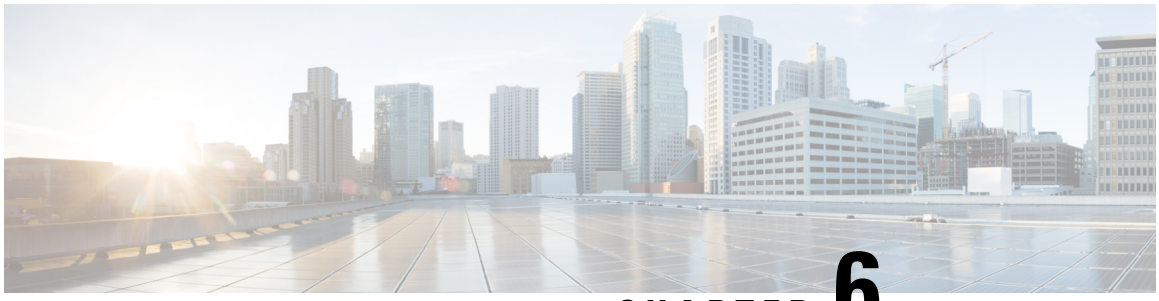
Verifying the Classification Configuration

Use the **show class-map** command to verify the class-map configuration. This command displays all class maps.

Configuration Examples for Classification

The following example shows how to configure classification for two classes of traffic:

```
class-map class_dscp
match dscp af21, af32
exit
class-map class_cos
match cos 4, 5-6
exit
```



CHAPTER 6

Configuring Marking

This chapter contains the following sections:

About Marking

Marking is a method that you use to modify the QoS fields of the incoming and outgoing packets. The QoS fields that you can mark are IP precedence and differentiated services code point (DSCP) in Layer 3. The QoS group is a label local to the system to which you can assign intermediate marking values. You can use the QoS group label to determine the egress scheduling.

You can use marking commands in traffic classes that are referenced in a policy map. The marking features that you can configure are listed in the following table:

Table 15: Configurable Marking Features

Marking Feature	Description
DSCP	Layer 3 DSCP.
IP precedence	Layer 3 IP precedence. **Note** IP precedence uses only the lower three bits of the type of service (ToS) field. The device overwrites the first three bits of the ToS field to 0.
QoS group	Locally significant QoS values that can be manipulated and matched within the system. The range is from 0 to 3.
Ingress	Status of the marking applies to incoming packets.

Marking Feature	Description
CoS	Layer 2 VLAN ID

Trust Boundaries

The trust boundary forms a perimeter on your network. Your network trusts (and does not override) the markings on your switch.

The incoming interface enforces the trust boundary as follows:

- All Fibre Channel and virtual Fibre Channel interfaces are automatically classified into the FCoE system class.
- By default, all Ethernet interfaces are trusted interfaces. A packet tagged with an 802.1p class of service (CoS) value is classified into a system class using the value in the packet.
- Any packet not tagged with an 802.1p CoS value is classified into the default drop system class. If the untagged packet is sent over a trunk, it is tagged with the default untagged CoS value, which is zero.
- You can override the default untagged CoS value for an Ethernet interface or port channel.

After the system applies the correct CoS value to an untagged packet, QoS treats the packet according to the newly defined class.

Class of Behavior

For routed unicast traffic, the CoS value is not available and the packet has the Differentiated Services Code Point (DSCP) value only. For bridged unicast traffic, the CoS value is copied from the CoS value received in the 802.1q header. Note that on Layer 2 access links there is no trunk header. Therefore, if traffic is received on an access port and bridged, it will egress the switch with CoS 0. The DSCP value does not change, but the packet may not get the desired priority. You can manually set the CoS value in a policy-map via any QoS policy that manually sets the CoS or DSCP value.

Routed multicast traffic derives its CoS value similar to routed unicast traffic. For bridged multicast traffic, the behavior depends on the Layer 3 state. If there is no Layer 3 state for the multicast group, the CoS is derived similar to the bridged unicast traffic. If there is a Layer 3 state for the multicast group, the CoS is derived similar to routed unicast traffic.

Note When you enable Protocol Independent Multicast (PIM) in sparse mode on the switch virtual interface (SVI) for the VLAN in which traffic is received, PIM creates an S,G entry for any multicast traffic.

Table 16: CoS Behavior per Traffic Type

Traffic Type	CoS Behavior
Routed unicast	Unchanged
Bridged unicast	Unchanged
Routed multicast	Copied from 3 MSB of ToS
Bridged multicast with Layer 3 state for group	Copied from 3 MSB of ToS

Bridged multicast with no Layer 3 state for group	Unchanged

Licensing Requirements for Marking

The following table shows the licensing requirements for this feature:

Product	License Requirement
Cisco NX-OS	The QoS feature does not a require license. Any feature not included in a license package is bundled with the NX-OS image and is provided at no extra charge to you. For a complete explanation of the Cisco NX-OS licensing scheme, see the *Cisco NX-OS Licensing Guide*.

Prerequisites for Marking

Classification has the following prerequisites:

- You must be familiar with using modular QoS CLI.
- You are logged on to the device.

Guidelines and Limitations for Marking

Marking has the following guidelines and limitations:

- Marking based on Egress policing result is not supported. For example:
  - **police percent 10 conform set-dscp-transmit 10 violate set-cos-transmit 5** is not supported.
  - **police percent 10 conform transmit violate drop** is supported.
- **show** commands with the **internal** keyword are not supported.
- The **set qos-group** command can only be used in ingress policies.

Note You can apply the marking instructions in a QoS policy map to ingress packets by attaching that QoS policy map to an interface. To select ingress, you specify the **input** keyword in the **service-policy** command.

For more information, see Attaching and Detaching a QoS Policy Action, on page 22.

- Control traffic, such as BPDUs, routing protocol packets, LACP/CDP/BFD, GOLD packets, glean traffic, and management traffic, are automatically classified into a control group, based on a criteria. These packets are classified into qos-group 7 and have a strict absolute priority over other traffic.

- Span traffic automatically gets classified into qos-group 0 and is scheduled at absolute low priority.
- QoS marking policies can be enabled on subinterfaces.
- Both CoS and DSCP/ToS values cannot be remarked for the same class of traffic.

Configuring Marking

You can combine one or more of the marking features in a policy map to control the setting of QoS values. You can then apply policies to either incoming or outgoing packets on an interface.

Note Do not press **Enter** after you use the **set** command and before you add the rest of the command. If you press **Enter** directly after entering the set keyword, you will be unable to continue to configure with the QoS configuration.

Configuring DSCP Marking

You can set the DSCP value in the six most significant bits of the DiffServ field of the IP header to a specified value. You can enter numeric values from 0 to 60, in addition to the standard DSCP values shown in the following table.

Table 17: Standard DSCP Values

Value	List of DSCP Values
af11	AF11 dscp (001010)—decimal value 10
af12	AF12 dscp (001100)—decimal value 12
af13	AF13 dscp (001110)—decimal value 14
af21	AF21 dscp (010010)—decimal value 18
af22	AF22 dscp (010100)—decimal value 20
af23	AF23 dscp (010110)—decimal value 22
af31	AF31 dscp (011010)—decimal value 26
af32	AF40 dscp (011100)—decimal value 28
af33	AF33 dscp (011110)—decimal value 30
af41	AF41 dscp (100010)—decimal value 34
af42	AF42 dscp (100100)—decimal value 36
af43	AF43 dscp (100110)—decimal value 38
cs1	CS1 (precedence 1) dscp (001000)—decimal value 8

Value	List of DSCP Values
cs2	CS2 (precedence 2) dscp (010000)—decimal value 16
cs3	CS3 (precedence 3) dscp (011000)—decimal value 24
cs4	CS4 (precedence 4) dscp (100000)—decimal value 32
cs5	CS5 (precedence 5) dscp (101000)—decimal value 40
cs6	CS6 (precedence 6) dscp (110000)—decimal value 48
cs7	CS7 (precedence 7) dscp (111000)—decimal value 56
default	Default dscp (000000)—decimal value 0
ef	EF dscp (101110)—decimal value 46

Note For more information about DSCP, see RFC 2475.

SUMMARY STEPS

1. **configure terminal**
2. **policy-map** [**type qos**] [**match-first**] *policy-map-name*
3. **class** [**type qos**] {*class-name* | **class-default**} [**insert-before** *before-class-name*]
4. **set dscp** *dscp-value*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `switch# configure terminal` `switch(config)#`	Enters global configuration mode.
Step 2	**policy-map** [**type qos**] [**match-first**] *policy-map-name* **Example:** `switch(config)# policy-map policy1` `switch(config-pmap-qos)#`	Creates or accesses the policy map named *policy-map-name* and then enters policy-map mode. The policy-map name can contain alphabetic, hyphen, or underscore characters, is case sensitive, and can be up to 40 characters.
Step 3	**class** [**type qos**] {*class-name* | **class-default**} [**insert-before** *before-class-name*] **Example:** `switch(config-pmap-qos)# class class1` `switch(config-pmap-c-qos)#`	Creates a reference to *class-name* and enters policy-map class configuration mode. The class is added to the end of the policy map unless **insert-before** is used to specify the class to insert before. Use the **class-default** keyword to select all traffic that is not currently matched by classes in the policy map.

	Command or Action	Purpose
Step 4	**set dscp** *dscp-value* **Example:** `switch(config-pmap-c-qos)# set dscp af31`	Sets the DSCP value to *dscp-value*. Standard values are shown in the previous Standard DSCP Values table. When the QoS policy is applied on the VLAN configuration level, the DSCP value derives the CoS value for bridged and routed traffic from the 3 most significant DSCP bits.

Example

This example shows how to display the policy-map configuration:

```
switch# show policy-map policy1
```

Configuring IP Precedence Marking

You can set the value of the IP precedence field in bits 0–2 of the IPv4 type of service (ToS) field of the IP header.

Note The device rewrites the last 3 bits of the ToS field to 0 for packets that match this class.

Table 18: Precedence Values

Value	List of Precedence Values
0-7	IP precedence value
critical	Critical precedence (5)
flash	Flash precedence (3)
flash-override	Flash override precedence (4)
immediate	Immediate precedence (2)
internet	Internetwork control precedence (6)
network	Network control precedence (7)
priority	Priority precedence (1)
routine	Routine precedence (0)

SUMMARY STEPS

1. **configure terminal**
2. **policy-map** [**type qos**] [**match-first**] *policy-map-name*
3. **class** [**type qos**] {*class-name* | **class-default**} [**insert-before** *before-class-name*]

4. **set precedence** *precedence-value*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `switch# configure terminal` `switch(config)#`	Enters global configuration mode.
Step 2	**policy-map** [**type qos**] [**match-first**] *policy-map-name* **Example:** `switch(config)# policy-map policy1` `switch(config-pmap-qos)#`	Creates or accesses the policy map named *policy-map-name* and then enters policy-map mode. The policy-map name can contain alphabetic, hyphen, or underscore characters, is case sensitive, and can be up to 40 characters.
Step 3	**class** [**type qos**] {*class-name* | **class-default**} [**insert-before** *before-class-name*] **Example:** `switch(config-pmap-qos)# class class1` `switch(config-pmap-c-qos)#`	Creates a reference to *class-name* and enters policy-map class configuration mode. The class is added to the end of the policy map unless **insert-before** is used to specify the class to insert before.
Step 4	**set precedence** *precedence-value* **Example:** `switch(config-pmap-c-qos)# set precedence 3`	Sets the IP precedence value to *precedence-value*. The value can range from 0 to 7. You can enter one of the values shown in the above Precedence Values table.

Example

This example shows how to display the policy-map configuration:

```
switch# show policy-map policy1
```

Configuring CoS Marking

You can set the value of the CoS field in the high-order three bits of the VLAN ID Tag field in the IEEE 802.1Q header.

SUMMARY STEPS

1. **configure terminal**
2. **policy-map** [**type qos**] [**match-first**] [*qos-policy-map-name* | **qos-dynamic**]
3. **class** [**type qos**] {*class-map-name* | **class-default**} [**insert-before** *before-class-name*]
4. **set cos** *cos-value*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `switch# configure terminal` `switch(config)#`	Enters global configuration mode.
Step 2	**policy-map** [**type qos**] [**match-first**] [*qos-policy-map-name* | **qos-dynamic**] **Example:** `switch(config)# policy-map policy1` `switch(config-pmap-qos)#`	Creates or accesses the policy map named *qos-policy-map-name*, and then enters policy-map mode. The policy-map name can contain alphabetic, hyphen, or underscore characters, is case sensitive, and can be up to 40 characters.
Step 3	**class** [**type qos**] {*class-map-name* | **class-default**} [**insert-before** *before-class-name*] **Example:** `switch(config-pmap-qos)# class class1` `switch(config-pmap-c-qos)#`	Creates a reference to *class-map-name*, and enters policy-map class configuration mode. The class is added to the end of the policy map unless **insert-before** is used to specify the class to insert before. Use the **class-default** keyword to select all traffic that is not currently matched by classes in the policy map.
Step 4	**set cos** *cos-value* **Example:** `switch(config-pmap-c-qos)# set cos 3` `switch(config-pmap-c-qos)#`	Sets the CoS value to *cos-value*. The value can range from 0 to 7.

Example

This example shows how to display the policy-map configuration:

```
switch# show policy-map policy1
```

Configuring DSCP Port Marking

You can set the DSCP value for each class of traffic defined in a specified ingress policy map.

The default behavior of the device is to preserve the DSCP value or to trust DSCP. To make the port untrusted, change the DSCP value. Unless you configure a QoS policy and attach that policy to specified interfaces, the DSCP value is preserved.

Note

- You can attach only one policy type qos map to each interface in each direction.
- The DSCP value is trust on the Layer 3 port of a Cisco NX-OS device.

SUMMARY STEPS

1. **configure terminal**

2. **policy-map** [**type qos**] [**match-first**] [*policy-map-name*]
3. **class** [**type qos**] {*class-name* | **class-default**} [**insert-before** *before-class-name*]
4. **set** *dscp-value*
5. **exit**
6. **class** [**type qos**] {*class-name* | **class-default**} [**insert-before** *before-class-name*]
7. **set** *dscp-value*
8. **exit**
9. **class** [**type qos**] {*class-name* | **class-default**} [**insert-before** *before-class-name*]
10. **set** *dscp-value*
11. **exit**
12. **interface ethernet** *slot/port*
13. **service-policy** [**type qos**] {**input** | **output**} {*policy-map-name*} [**no-stats**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `switch# configure terminal` `switch(config)#`	Enters global configuration mode.
Step 2	**policy-map** [**type qos**] [**match-first**] [*policy-map-name*] **Example:** `switch(config)# policy-map policy1` `switch(config-pmap-qos)#`	Creates or accesses the policy map named *policy-map-name* and then enters policy-map mode. The policy-map name can contain alphabetic, hyphen, or underscore characters, is case sensitive, and can be up to 40 characters.
Step 3	**class** [**type qos**] {*class-name*	**class-default**} [**insert-before** *before-class-name*] **Example:** `switch(config-pmap-qos)# class class1` `switch(config-pmap-c-qos)#`	Creates a reference to *class-name* and enters policy-map class configuration mode. The class is added to the end of the policy map unless **insert-before** is used to specify the class to insert before. Use the **class-default** keyword to select all traffic that is not currently matched by classes in the policy map.
Step 4	**set** *dscp-value* **Example:** `switch(config-pmap-c-qos)# set dscp af31`	Sets the DSCP value to dscp-value. Valid values are listed in the Standard DSCP Values table in the Configuring DSCP Marking section.
Step 5	**exit** **Example:** `switch(config-pmap-c-qos)# exit` `switch(config-pmap-qos)#`	Returns to policy-map configuration mode.
Step 6	**class** [**type qos**] {*class-name*	**class-default**} [**insert-before** *before-class-name*] **Example:** `switch(config-pmap-qos)# class class2` `switch(config-pmap-c-qos)#`	Creates a reference to *class-name* and enters policy-map class configuration mode. The class is added to the end of the policy map unless **insert-before** is used to specify the class to insert before. Use the **class-default** keyword to select all traffic that is not currently matched by classes in the policy map.

	Command or Action	Purpose
Step 7	**set** *dscp-value* **Example:** `switch(config-pmap-c-qos)# set dscp af1`	Sets the DSCP value to dscp-value. Valid values are listed in the Standard DSCP Values table in the Configuring DSCP Marking section.
Step 8	**exit** **Example:** `switch(config-pmap-c-qos)# exit` `switch(config-pmap-qos)#`	Returns to policy-map configuration mode.
Step 9	**class** [**type qos**] {*class-name* | **class-default**} [**insert-before** *before-class-name*] **Example:** `switch(config-pmap-qos)# class class-default` `switch(config-pmap-c-qos)#`	Creates a reference to *class-name* and enters policy-map class configuration mode. The class is added to the end of the policy map unless **insert-before** is used to specify the class to insert before. Use the **class-default** keyword to select all traffic that is not currently matched by classes in the policy map.
Step 10	**set** *dscp-value* **Example:** `switch(config-pmap-c-qos)# set dscp af22` `switch(config-pmap-c-qos)#`	Sets the DSCP value to dscp-value. Valid values are listed in the Standard DSCP Values table in the Configuring DSCP Marking section.
Step 11	**exit** **Example:** `switch(config-pmap-c-qos)# exit` `switch(config-pmap-qos)#`	Returns to policy-map configuration mode.
Step 12	**interface ethernet** *slot/port* **Example:** `switch(config)# interface ethernet 1/1` `switch(config-if)#`	Enters interface mode to configure the Ethernet interface.
Step 13	**service-policy** [**type qos**] {**input** | **output**} {*policy-map-name*} [**no-stats**] **Example:** `switch(config-if)# service-policy input policy1`	Adds *policy-map-name* to the input packets of the interface. You can attach only one input policy and one output policy to an interface.

Example

This example shows how to display the policy-map configuration:

```
switch# show policy-map policy1
```

Verifying the Marking Configuration

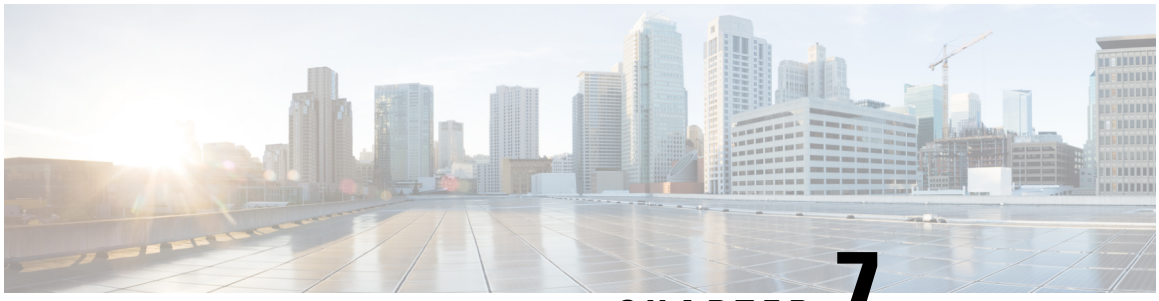
To display the marking configuration information, perform one of the following tasks:

Command	Purpose
show policy-map	Displays all policy maps.

Configuration Examples for Marking

The following example shows how to configure marking:

```
configure terminal
policy-map type qos untrust_dcsp
class class-default
set precedence 3
set qos-qroup 3
set dscp 0
```



CHAPTER 7

Configuring Policing

This chapter contains the following sections:

About Policing

Policing is the monitoring of the data rates for a particular class of traffic. When the data rate exceeds user-configured values, marking or dropping of packets occurs immediately. Policing does not buffer the traffic; therefore, the transmission delay is not affected. When traffic exceeds the data rate, you instruct the system to either drop the packets or mark QoS fields in them.

You can define single-rate and dual-rate policers. Single-rate policers monitor the committed information rate (CIR) of traffic.

You can configure only one action for each condition. For example, you might police for traffic in a class to conform to the data rate of 256000 bits per second, with up to 200 millisecond bursts. The system would apply the conform action to traffic that falls within this rate, and it would apply the violate action to traffic that exceeds this rate.

For more information about policers, see RFC 2697 and RFC 2698.

Licensing Requirements for Policing

The following table shows the licensing requirements for this feature:

Product	License Requirement
Cisco NX-OS	The QoS feature does not a require license. Any feature not included in a license package is bundled with the NX-OS image and is provided at no extra charge to you. For a complete explanation of the Cisco NX-OS licensing scheme, see the Cisco NX-OS Licensing Guide.

Prerequisites for Policing

Policing has the following prerequisites:

- You must be familiar with using modular QoS CLI.
- You are logged on to the device.

Guidelines and Limitations for Policing

Policing has the following guidelines and limitations:

Common

The following are guidelines and limitations common to all policers:

- **show** commands with the **internal** keyword are not supported.
- Each slice applies policing independently, which can affect QoS features that are applied to traffic that is distributed across multiple modules. The following are examples of these QoS features:
  - Policers that are applied to a port channel interface.
  - Policers that are applied to a VLAN.
- Using the optional keyword, **no-stats** disables statistics and ensures that applicable policies are shared.
- You can only use the **set qos-group** command in ingress policies.
- Policer rate may less than configured value. There can be a slight difference between the configured rate and actual applied rate.

Ingress Policing

The following are guidelines and limitations for ingress policing:

- All policers in the ingress direction must use the same mode.
- QoS Ingress policers can be enabled on subinterfaces.

Egress Policing

The following are guidelines and limitations for egress policing:

- Policing counters for different colors are not supported. There is only a single hit counter for TCAM entry.
- Egress QoS policies are not supported on subinterfaces.
- Egress policers with remarking action are not supported.

1-Rate and 2-Rate, 2-Color and 3-Color Policing

The following are guidelines and limitations for 1-Rate and 2-Rate, 2-Color and 3-Color policing:

- 2-rate 3-color policing is not supported (only 1 rate 2 color policers are supported).

Configuring Policing

You can configure a single or dual-rate policer.

Configuring Ingress Policing

You can apply the policing instructions in a QoS policy map to ingress packets by attaching that QoS policy map to an interface. To select ingress, you specify the **input** keyword in the **service-policy** command. For more information on attaching and detaching a QoS policy action from an interface, see the "Using Modular QoS CLI" section.

Configuring 1-Rate and 2-Color Policing

The type of policer created by the device is based on a combination of the **police** command arguments described in the following Arguments to the police Command table.

Note You must specify the identical value for **pir** and **cir** to configure 1-rate 2-color policing.

Note A 1-rate 2-color policer with the violate markdown action is not supported.

Table 19: Arguments to the Police Command

Argument	Description
cir	Committed information rate, or desired bandwidth, specified as a bit rate or a percentage of the link rate. Although a value for cir is required, the argument itself is optional. The range of values is from 1 to 80000000000. The range of policing values is from 8000 to 80 Gbps.

Argument	Description
percent	Rate as a percentage of the interface rate. The range of values is from 1 to 100 percent.
bc	Indication of how much the cir can be exceeded, either as a bit rate or an amount of time at cir. The default is 200 milliseconds of traffic at the configured rate. The default data rate units are bytes.
pir	Peak information rate, specified as a PIR bit rate or a percentage of the link rate. There is no default. The range of values is from 1 to 80000000000; the range of policing values is from 8000 bps to 480 Gbps. The range of percentage values is from 1 to 100 percent.
be	Indication of how much the pir can be exceeded, either as a bit rate or an amount of time at pir. When the bc value is not specified, the default is 200 milliseconds of traffic at the configured rate. The default data rate units are bytes. **Note** You must specify a value for pir before the device displays this argument.
conform	Single action to take if the traffic data rate is within bounds. The basic actions are transmit or one of the set commands listed in the following Policer Actions for Conform table. The default is transmit.
exceed	Single action to take if the traffic data rate is exceeded. The basic actions are drop or markdown. The default is drop.
violate	Single action to take if the traffic data rate violates the configured rate values. The basic actions are drop or markdown. The default is drop.

Although all the arguments in the above Arguments to the police Command table are optional, you must specify a value for **cir**. In this section, **cir** indicates its value but not necessarily the keyword itself. The combination of these arguments and the resulting policer types and actions are shown in the following Policer Types and Actions from Police Arguments Present table.

Table 20: Policer Types and Actions from Police Arguments Present

Police Arguments Present	Policer Type	Policer Action
cir, but not **pir**, **be**, or **violate**	1-rate, 2-color	<= **cir**, **conform**; else **violate**

The policer actions that you can specify are described in the following Policer Actions for Exceed or Violate table and the following Policer Actions for Conform table.

Table 21: Policer Actions for Exceed or Violate

Action	Description
drop	Drops the packet. This action is available only when the packet exceeds or violates the parameters.
set-cos-transmit	Sets CoS and transmits the packet.
set-dscp-transmit	Sets DSCP and transmits the packet.

Action	Description
set-prec-transmit	Sets precedence and transmits the packet.
set-qos-transmit	Sets qos-group and transmits the packet.

Table 22: Policer Actions for Conform

Action	Description
transmit	Transmits the packet. This action is available only when the packet conforms to the parameters.
set-prec-transmit	Sets the IP precedence field to a specified value and transmits the packet. This action is available only when the packet conforms to the parameters.
set-dscp-transmit	Sets the differentiated service code point (DSCP) field to a specified value and transmits the packet. This action is available only when the packet conforms to the parameters.
set-cos-transmit	Sets the class of service (CoS) field to a specified value and transmits the packet. This action is available only when the packet conforms to the parameters.
set-qos-transmit	Sets the QoS group internal label to a specified value and transmits the packet. This action can be used only in input policies and is available only when the packet conforms to the parameters.

Note The policer can only drop or mark down packets that exceed or violate the specified parameters. For information on marking down packets, see the Configuring Marking, on page 50 section.

The data rates used in the **police** command are described in the following Data Rates for the police Command table.

Table 23: Data Rates for the police Command

Rate	Description
bps	Bits per second (default)
kbps	1,000 bits per seconds
mbps	1,000,000 bits per second
gbps	1,000,000,000 bits per second

Burst sizes used in the **police** command are described in the following Burst Sizes for the police Command table.

Table 24: Burst Sizes for the police Command

Speed	Description
bytes	bytes
kbytes	1,000 bytes
mbytes	1,000,000 bytes
ms	milliseconds
us	microseconds

.

SUMMARY STEPS

1. **configure terminal**
2. **policy-map** [**type qos**] [**match-first**] [*policy-map-name*]
3. **class** [**type qos**] {*class-map-name* | **class-default**} [**insert-before** *before-class-name*]
4. **police** [**cir**] {*committed-rate* [*data-rate*] | **percent** *cir-link-percent*} [**bc** *committed-burst-rate* [*link-speed*]][**pir**] {*peak-rate* [*data-rate*] | **percent** *cir-link-percent*} [**be** *peak-burst-rate* [*link-speed*]] [**conform** {**transmit** | **set-prec-transmit** | **set-dscp-transmit** | **set-cos-transmit** | **set-qos-transmit**} [**exceed** {**drop**} [**violate** {**drop** | **set-cos-transmit** | **set-dscp-transmit** | **set-prec-transmit** | **set-qos-transmit**}]]}
5. [violate {**drop** | **set-cos-transmit** | **set-dscp-transmit** | **set-prec-transmit** | **set-qos-transmit**}]
6. **exit**
7. **exit**
8. **show policy-map** [**type qos**] [*policy-map-name* | **qos-dynamic**]
9. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `switch# configure terminal` `switch(config)#`	Enters global configuration mode.
Step 2	**policy-map** [**type qos**] [**match-first**] [*policy-map-name*] **Example:** `switch(config)# policy-map policy1` `switch(config-pmap-qos)#`	Creates or accesses the policy map named *policy-map-name* and then enters policy-map mode. The policy-map name can contain alphabetic, hyphen, or underscore characters, is case sensitive, and can be up to 40 characters.
Step 3	**class** [**type qos**] {*class-map-name*	**class-default**} [**insert-before** *before-class-name*] **Example:** `switch(config-pmap-qos)# class class-default` `switch(config-pmap-c-qos)#`	Creates a reference to *class-map-name* and enters policy-map class configuration mode. The class is added to the end of the policy map unless **insert-before** is used to specify the class to insert before. Use the **class-default**

	Command or Action	Purpose
		keyword to select all traffic that is not currently matched by classes in the policy map.
Step 4	**police** [**cir**] {*committed-rate* [*data-rate*] | **percent** *cir-link-percent*} [**bc** *committed-burst-rate* [*link-speed*]][**pir**] {*peak-rate* [*data-rate*] | **percent** *cir-link-percent*} [**be** *peak-burst-rate* [*link-speed*]] [**conform** {**transmit** | **set-prec-transmit** | **set-dscp-transmit** | **set-cos-transmit** | **set-qos-transmit**} [**exceed** {**drop**} [**violate** {**drop** | **set-cos-transmit** | **set-dscp-transmit** | **set-prec-transmit** | **set-qos-transmit**}]]}	Polices **cir** in bits or as a percentage of the link rate. The **conform** action is taken if the data rate is <= cir. If **be** and **pir** are not specified, all other traffic takes the **violate** action. If **be** or **violate** are specified, the **exceed** action is taken if the data rate <= **pir**, and the **violate** action is taken otherwise. The actions are described in the Policer Actions for Exceed or Violate table and the Policer Actions for Conform table. The data rates and link speeds are described in the Data Rates for the police Command table and the Burst Sizes for the police Command table.
Step 5	[violate {**drop** | **set-cos-transmit** | **set-dscp-transmit** | **set-prec-transmit** | **set-qos-transmit**}]	**set-cos-transmit**—Set cos and send it. **set-dscp-transmit**—Set dscp and send it. **set-prec-transmit**—Set precedence and send it. **set-qos-transmit**—Set qos-group and send it.
Step 6	**exit** **Example:** `switch(config-pmap-c-qos)# exit` `switch(config-pmap-qos)#`	Exits policy-map class configuration mode and enters policy-map mode.
Step 7	**exit** **Example:** `switch(config-pmap-qos)# exit` `switch(config)#`	Exits policy-map mode and enters global configuration mode.
Step 8	**show policy-map** [**type qos**] [*policy-map-name* | **qos-dynamic**] **Example:** `switch(config)# show policy-map`	(Optional) Displays information about all configured policy maps or a selected policy map of type qos.
Step 9	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	(Optional) Saves the running configuration to the startup configuration.

Example

This example shows how to display the policy1 policy-map configuration:

```
switch# show policy-map policy1
```

Configuring Markdown Policing

Markdown policing is the setting of a QoS field in a packet when traffic exceeds or violates the policed data rates. You can configure markdown policing by using the set commands for policing action described in the Policer Actions for Exceed or Violate table and the Policer Actions for Conform table.

SUMMARY STEPS

1. **configure terminal**
2. **policy-map** [**type qos**] [**match-first**] [*policy-map-name*]
3. **class** [**type qos**] {*class-name* | **class-default**} [**insert-before** *before-class-name*]
4. **police** [**cir**] {*committed-rate* [*data-rate*] | **percent** *cir-link-percent*} [[**bc** | **burst**] *burst-rate* [*link-speed*]] [[**be** | **peak-burst**] *peak-burst-rate* [*link-speed*]] [**conform** *conform-action* [**exceed** [**violate drop set dscp dscp table** *pir-markdown-map*]]}
5. **exit**
6. **exit**
7. **show policy-map** [**type qos**] [*policy-map-name*]
8. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `switch# configure terminal` `switch(config)#`	Enters global configuration mode.
Step 2	**policy-map** [**type qos**] [**match-first**] [*policy-map-name*] **Example:** `switch(config)# policy-map policy1` `switch(config-pmap-qos)#`	Creates or accesses the policy map named *policy-map-name* and then enters policy-map mode. The policy-map name can contain alphabetic, hyphen, or underscore characters, is case sensitive, and can be up to 40 characters.
Step 3	**class** [**type qos**] {*class-name* | **class-default**} [**insert-before** *before-class-name*] **Example:** `switch(config-pmap-qos)# class class-default` `switch(config-pmap-c-qos)#`	Creates a reference to *class-name* and enters policy-map class configuration mode. The class is added to the end of the policy map unless **insert-before** is used to specify the class to insert before. Use the **class-default** keyword to select all traffic that is not currently matched by classes in the policy map.
Step 4	**police** [**cir**] {*committed-rate* [*data-rate*] | **percent** *cir-link-percent*} [[**bc** | **burst**] *burst-rate* [*link-speed*]] [[**be** | **peak-burst**] *peak-burst-rate* [*link-speed*]] [**conform** *conform-action* [**exceed** [**violate drop set dscp dscp table** *pir-markdown-map*]]}	Polices **cir** in bits or as a percentage of the link rate. The **conform** action is taken if the data rate is <= cir. If **be** and **pir** are not specified, all other traffic takes the **violate** action. If **be** or **violate** are specified, the **exceed** action is taken if the data rate <= **pir**, and the **violate** action is taken otherwise. The actions are described in the Policer Actions for Exceed or Violate table and the Policer Actions for Conform table. The data rates and link speeds are described in the Data Rates for the police Command table and the Burst Sizes for the police Command table.

	Command or Action	Purpose
Step 5	**exit** **Example:** `switch(config-pmap-c-qos)# exit` `switch(config-pmap-qos)#`	Exits policy-map class configuration mode and enters policy-map mode.
Step 6	**exit** **Example:** `switch(config-pmap-qos)# exit` `switch(config)#`	Exits policy-map mode and enters global configuration mode.
Step 7	**show policy-map** [**type qos**] [*policy-map-name*] **Example:** `switch(config)# show policy-map`	(Optional) Displays information about all configured policy maps or a selected policy map of type qos.
Step 8	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	(Optional) Saves the running configuration to the startup configuration.

Verifying the Policing Configuration

To display the policing configuration information, perform one of the following tasks:

Command	Purpose
show policy-map	Displays information about policy maps and policing.

Configuration Examples for Policing

The following example shows how to configure policing for a 1-rate, 2-color policer:

```
configure terminal
  policy-map policy1
    class one_rate_2_color_policer
      police cir 256000 conform transmit violate drop
```

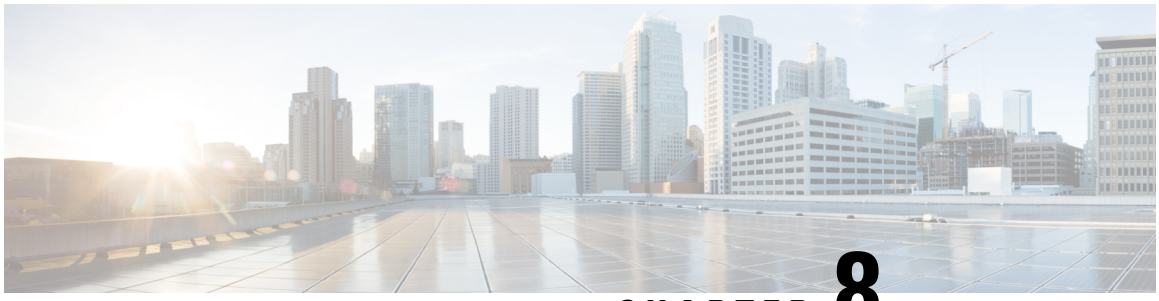
The following example shows how to configure policing for a 1-rate, 2-color policer with DSCP markdown:

```
configure terminal
  policy-map policy2
    class one_rate_2_color_policer_with_dscp_markdown
      police cir 256000 conform transmit violate drop
```

The following example shows how to configure policing for a shared policer:

```
configure terminal
 qos shared-policer type qos udp_10mbps cir 10 mbps pir 20 mbps conform transmit exceed
set dscp dscp table cir-markdown-map violate drop
 policy-map type qos udp_policy
```

```
class type qos udp_qos
 police aggregate udp_10mbps
```



CHAPTER 8

Configuring Queuing and Scheduling

This chapter contains the following sections:

About Queuing and Scheduling

Traffic queuing is the ordering of packets and applies to both input and output of data. Device modules can support multiple queues, which you can use to control the sequencing of packets in different traffic classes. You can also set weighted random early detection (WRED) and taildrop thresholds. The device drops packets only when the configured thresholds are exceeded.

Traffic scheduling is the methodical output of packets at a desired frequency to accomplish a consistent flow of traffic. You can apply traffic scheduling to different traffic classes to weight the traffic by priority.

The queuing and scheduling processes allow you to control the bandwidth that is allocated to the traffic classes so that you achieve the desired trade-off between throughput and latency for your network.

Modifying Class Maps

System-defined queuing class maps are provided.

Note The provided system-defined queuing class maps cannot be modified.

Congestion Avoidance

You can use the following methods to proactively avoid traffic congestion on the device:

- Apply WRED to TCP or non-TCP traffic.
- Apply tail drop to TCP or non-TCP traffic.

Congestion Management

For egress packets, you can choose one of the following congestion management methods:

- Specify a bandwidth that allocates a minimum data rate to a queue.
- Impose a minimum and maximum data rate on a class of traffic so that excess packets are retained in a queue to shape the output rate.
- Allocate all data for a class of traffic to a priority queue. The device distributes the remaining bandwidth among the other queues.

For information about configuring congestion management, see the Configuring WRED on Egress Queues section.

Explicit Congestion Notification

ECN is an extension to WRED that marks packets instead of dropping them when the average queue length exceeds a specific threshold value. When configured with the WRED ECN feature, routers and end hosts use this marking as a signal that the network is congested to slow down sending packets.

Note Enabling WRED and ECN on a class on a system-qos policy implies that WRED and ECN is enabled for all ports in the system.

Traffic Shaping

Traffic shaping allows you to control the traffic going out of an interface in order to match its flow to the speed of the remote target interface and to ensure that the traffic conforms to policies contracted for it. You can shape traffic that adheres to a particular profile to meet downstream requirements. Traffic shaping eliminates bottlenecks in topologies with data-rate mismatches.

Traffic shaping regulates and smooths out the packet flow by imposing a maximum traffic rate for each port's egress queue. Packets that exceed the threshold are placed in the queue and are transmitted later. Traffic shaping is similar to traffic policing, but the packets are not dropped. Because packets are buffered, traffic shaping minimizes packet loss (based on the queue length), which provides better traffic behavior for TCP traffic.

Using traffic shaping, you can control access to available bandwidth, ensure that traffic conforms to the policies established for it, and regulate the flow of traffic to avoid congestion that can occur when the egress traffic exceeds the access speed of its remote, target interface. For example, you can control access to the bandwidth when policy dictates that the rate of a given interface should not, on average, exceed a certain rate even though the access rate exceeds the speed.

Queue length thresholds are configured using the WRED configuration.

Licensing Requirements for Queuing and Scheduling

The following table shows the licensing requirements for this feature:

Product	License Requirement
Cisco NX-OS	The QoS feature does not a require license. Any feature not included in a license package is bundled with the NX-OS image and is provided at no extra charge to you. For a complete explanation of the Cisco NX-OS licensing scheme, see the Cisco NX-OS Licensing Guide.

Prerequisites for Queuing and Scheduling

Queuing and scheduling have the following prerequisites:

- You must be familiar with using modular QoS CLI.
- You are logged on to the device.

Guidelines and Limitations for Queuing and Scheduling

Queuing and scheduling has the following guidelines and limitations:

- Egress queue drop bytes information is an approximate calculation based on the number of cells used.
- WRED burst optimized and mesh optimized configurations are not supported.

- **show** commands with the **internal** keyword are not supported.
- Approximate Fair Drop (AFD) is not supported.
- Beginning with NX-OS release 9.2(2v), ingress queuing is supported.
- The device supports a system-level queuing policy, so all ports in the system are impacted when you configure the queuing policy.
- The device supports eight (8) egress queues on each port. There is not a separate queue for multicast or CPU traffic because they share the existing 8 queues. Both unicast and non-unicast traffic share the same egress queue.
- Control packets by default share q7 while Span packets use default q0.
- A type queuing policy can be attached to the system or to individual interfaces for output traffic.
- Changes are disruptive. The traffic passing through ports of the specified port type experience a brief period of traffic loss. All ports of the specified type are affected.
- Performance can be impacted. If one or more ports of the specified type do not have a queuing policy applied that defines the behavior for the new queue, the traffic mapping to that queue can experience performance degradation.
- Traffic shaping can increase the latency of packets due to queuing because it falls back to store-and-forward mode when packets are queued.
- When configuring priority for one class map queue (SPQ), configure the priority for QoS group 7. When configuring priority for more than one class map queue, configure the priority on the higher numbered QoS groups. In addition, the QoS groups must be next to each other. For example, if you want to have two SPQs, you have to configure the priority on QoS group 7 and on QoS group 6.
- WRED is applicable only for TCP or UDP packets.
- The maximum threshold for WRED must be equal to, or greater than, n times the minimum.
- WRED statistics are supported per-port. Per-queue WRED statistics are not supported.

Configuring Queuing and Scheduling

Queuing and scheduling are configured by creating policy maps of type queuing that you apply to an egress interface. You can modify system-defined class maps, which are used in policy maps to define the classes of traffic to which you want to apply policies.

For information about configuring policy maps and class maps, see the "Using Modular QoS CLI" section.

You can configure the congestion-avoidance features, which include tail drop and WRED, in any queue.

You can configure one of the egress congestion management features, such as priority, traffic shaping, and bandwidth in output queues.

The system-defined policy map, default-out-policy, is attached to all ports to which you do not apply a queuing policy map. The default policy maps cannot be configured.

Configuring Type Queuing Policies

Type queuing policies for egress are used for scheduling and buffering the traffic of a specific system class. A type queuing policy is identified by its QoS group and can be attached to the system or to individual interfaces for input or output traffic.

Note Ingress queuing policy is used to configure pause buffer thresholds. For more details, see the About Priority Flow Control section.

SUMMARY STEPS

1. **configure terminal**
2. **policy-map type queuing** *policy-name*
3. **class type queuing** *class-name*
4. **priority**
5. **no priority**
6. **shape** {**kbps** | **mbps** | **gbps**} *burst size* **min** *minimum bandwidth*
7. **bandwidth percent** *percentage*
8. (Optional) **no bandwidth percent** *percentage*
9. (Optional) **priority level** *level*
10. (Optional) **queue-limit** *queue size* [**dynamic** *dynamic threshold*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**policy-map type queuing** *policy-name*	Creates a named object that represents a set of policies that are to be applied to a set of traffic classes. Policy-map names can contain alphabetic, hyphen, or underscore characters, are case sensitive, and can be up to 40 characters.
Step 3	**class type queuing** *class-name*	Associates a class map with the policy map, and enters configuration mode for the specified system class.
Step 4	**priority**	Specifies that traffic in this class is mapped to a strict priority queue.
Step 5	**no priority**	(Optional) Removes the strict priority queuing from the traffic in this class.
Step 6	**shape** {**kbps** | **mbps** | **gbps**} *burst size* **min** *minimum bandwidth*	Specifies the burst size and minimum guaranteed bandwidth for this queue.
Step 7	**bandwidth percent** *percentage*	Assigns a weight to the class. The class will receive the assigned percentage of interface bandwidth if there are no strict-priority queues. If there are strict-priority queues,

	Command or Action	Purpose
		however, the strict-priority queues receive their share of the bandwidth first. The remaining bandwidth is shared in a weighted manner among the class configured with a bandwidth percent. For example, if strict-priority queues take 90 percent of the bandwidth, and you configure 75 percent for a class, the class will receive 75 percent of the remaining 10 percent of the bandwidth. **Note** Before you can successfully allocate bandwidth to the class, you must first reduce the default bandwidth configuration on class-default and class-fcoe.
Step 8	(Optional) **no bandwidth percent** *percentage*	Removes the bandwidth specification from this class.
Step 9	(Optional) **priority level** *level*	Specifies the strict priority levels for the Cisco Nexus 3400-S switches. These levels can be 1, 2, or 3.
Step 10	(Optional) **queue-limit** *queue size* [**dynamic** *dynamic threshold*]	Specifies either the static or dynamic shared limit available to the queue for Cisco Nexus 3400-S switches. The static queue limit defines the fixed size to which the queue can grow. The dynamic queue limit allows the queue's threshold size to be decided depending on the number of free cells available, in terms of the alpha value.

Configuring Congestion Avoidance

You can configure congestion avoidance with tail drop or WRED features. Both features can be used in egress policy maps.

Configuring Tail Drop on Egress Queues

You can configure tail drop on egress queues by setting thresholds. The device drops any packets that exceed the thresholds. You can specify a threshold that is based on the queue size or buffer memory that is used by the queue.

SUMMARY STEPS

1. **configure terminal**
2. **policy-map** [**type queuing**] [**match-first**] [*policy-map-name*]
3. **class type queuing** *class-name*
4. **queue-limit** {*queue-size* [**bytes** | **kbytes** | **mbytes**] | **dynamic** *value*}
5. (Optional) Repeat Steps 3 and 4 to assign tail drop thresholds for other queue classes.
6. **show policy-map** [**type queuing** [*policy-map-name* | **default-8q-out-policy**]]
7. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `switch# configure terminal` `switch(config)#`	Enters global configuration mode.
Step 2	**policy-map** [**type queuing**] [**match-first**] [*policy-map-name*] **Example:** `switch(config)# policy-map type queuing shape_queues` `switch(config-pmap-que)#`	Configures the policy map of type queuing and then enters policy-map mode for the policy-map name you specify. Policy-map names can contain alphabetic, hyphen, or underscore characters, are case-sensitive, and can be up to 40 characters.
Step 3	**class type queuing** *class-name* **Example:** `switch(config-pmap-que)# class type queuing c-out-q1` `switch(config-pmap-c-que)#`	Configures the class map of type queuing and then enters policy-map class queuing mode. Class queuing names are listed in the previous System-Defined Type queuing Class Maps table.
Step 4	**queue-limit** {*queue-size* [**bytes** | **kbytes** | **mbytes**] | **dynamic** *value*} **Example:** `switch(config-pmap-c-que)# queue-limit 1000 mbytes`	Assigns a tail drop threshold that is based on the queue size in bytes, kilobytes, or megabytes or allows the queue's threshold size to be determined dynamically depending on the number of free cells available. The device drops packets that exceed the specified threshold. The Cisco Nexus 3400-S switches use a single egress queue for sending both unicast and non-unicast traffic. The buffer utilization for the respective traffic is defined by alpha values that are different for unicast and non-unicast. Queue limit changes affect only the unicast alpha values.

Value of queue limit/alpha	Unicast definition	Multicast definition	Max % per queue
1	1/16	1/4	~6%
2	1/8	1/4	~11%
3	1/4	1/4	20%
4	1/2	1/4	~33%
5	1	1/4	50%
6	2	1/4	~67%
7	4	1/4	80%
8	8	1/4	~89%

	Command or Action	Purpose
		For example, if you configure a dynamic queue size of 6, then the alpha value is ½. If you configure a dynamic queue size of 7, then the alpha value is 1. To calculate the queue-limit, consider the following: queue-limit = (alpha/(1 + alpha)) x total buffers For example, if you configure a queue-limit with a dynamic queue size of 7, then the queue-limit can grow up to (1/(1+1)) x total buffers. This means that the queue-limit = ½ x total buffers.
Step 5	(Optional) Repeat Steps 3 and 4 to assign tail drop thresholds for other queue classes.	
Step 6	**show policy-map** [**type queuing** [*policy-map-name* | **default-8q-out-policy**]] **Example:** `switch(config-pmap-c-que)# show policy-map type queuing shape_queues`	(Optional) Displays information about all configured policy maps, all policy maps of type queuing, a selected policy map of type queuing, or the default output queuing policy.
Step 7	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	(Optional) Saves the running configuration to the startup configuration.

Configuring WRED on Egress Queues

You can configure WRED on egress queues to set minimum and maximum packet drop thresholds. The frequency of dropped packets increases as the queue size exceeds the minimum threshold. When the maximum threshold is exceeded, all packets for the queue are dropped.

SUMMARY STEPS

1. **configure terminal**
2. **policy-map type queuing** {[**match-first**] *policy-map-name*}
3. **class type queuing** *class-name*
4. **random-detect** [**minimum-threshold** *min-threshold* {**packets** | **bytes** | **kbytes** | **mbytes**} **maximum-threshold** *max-threshold* {**packets** | **bytes** | **kbytes** | **mbytes**} **drop-probability** *value* **weight** *value*] [**ecn** | **non-ecn**]
5. (Optional) Repeat Steps 3 and 4 to configure WRED for other queuing classes.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`switch# configure terminal` `switch(config)#`	
Step 2	**policy-map type queuing** {[**match-first**] *policy-map-name*} **Example:** `switch(config)# policy-map type queuing p1` `switch(config-pmap-que)#`	Configures the policy map of type queuing and then enters policy-map mode for the policy-map name you specify. Policy-map names can contain alphabetic, hyphen, or underscore characters, are case-sensitive, and can be up to 40 characters.
Step 3	**class type queuing** *class-name* **Example:** `switch(config-pmap-que)# class type queuing c-out-q1` `switch(config-pmap-c-que)#`	Configures the class map of type queuing and then enters policy-map class queuing mode. Class queuing names are listed in the previous System-Defined Type queuing Class Maps table.
Step 4	**random-detect** [**minimum-threshold** *min-threshold* {**packets** | **bytes** | **kbytes** | **mbytes**} **maximum-threshold** *max-threshold* {**packets** | **bytes** | **kbytes** | **mbytes**} **drop-probability** *value* **weight** *value*] [**ecn** | **non-ecn**] **Example:** `switch(config-pmap-c-que)# random-detect minimum-threshold 10 mbytes maximum-threshold 20 mbytes` **Example:** `switch(config-pmap-c-que)# random-detect non-ecn minimum-threshold 1000 kbytes maximum-threshold 4000 kbytes drop-probability 100` `switch# show queuing interface e1/1  | i WRED|AQM` `| WRED/AQM & Tail Drop Pkts |       0 |` `| WRED/AQM & Tail Drop Byts |       0 |` `| WRED/AQM & Tail Drop Pkts |       0 |` `| WRED/AQM & Tail Drop Byts |       0 |` `| WRED/AQM & Tail Drop Pkts |       0 |` `| WRED/AQM & Tail Drop Byts |       0 |` `| WRED/AQM & Tail Drop Pkts |       0 |` `| WRED/AQM & Tail Drop Byts |       0 |` `| WRED/AQM & Tail Drop Pkts |       0 |` `| WRED/AQM & Tail Drop Byts |       0 |` `| WRED/AQM & Tail Drop Pkts |       0 |` `| WRED/AQM & Tail Drop Byts |       0 |` `| WRED/AQM & Tail Drop Pkts |       0 |`	Configures WRED on the specified queuing class. You can specify minimum and maximum thresholds that are used to drop packets from the queue. You can configure these thresholds by the number of packets, bytes, kilobytes, or megabytes. The minimum and maximum thresholds must be of the same type. The thresholds are from 1 to 52428800. Alternatively, you can configure WRED to drop packets that are based on explicit congestion notification (ECN). The Network Forwarding Engine (NFE) platform supports the **non-ecn** option to configure drop thresholds for non-ECN flows.

	Command or Action	Purpose
	<pre>| WRED/AQM & Tail Drop Byts | 0 | | WRED/AQM & Tail Drop Pkts | 0 | | WRED/AQM & Tail Drop Byts | 0 | | Green WRED/AQM Drops (Pkts) | 0 | | Yellow WRED/AQM Drops (Pkts) | 0 | | Red WRED/AQM Drops (Pkts) | 0</pre>	
Step 5	(Optional) Repeat Steps 3 and 4 to configure WRED for other queuing classes.	

Configuring Congestion Management

You can configure only one of the following congestion management methods in a policy map:

- Allocate a minimum data rate to a queue by using the **bandwidth** and **bandwidth remaining** commands.
- Allocate all data for a class of traffic to a priority queue by using the **priority** command. You can use the **bandwidth remaining** command to distribute remaining traffic among the nonpriority queues. By default, the system evenly distributes the remaining bandwidth among the nonpriority queues.
- Allocate a minimum and maximum data rate to a queue by using the **shape** command.

In addition to the congestion management feature that you choose, you can configure one of the following queue features in each class of a policy map:

- Taildrop thresholds based on the queue size and the queue limit usage. For more information, see the section.

  Configuring Tail Drop on Egress Queues, on page 74
- WRED for preferential packet drops. For more information, see the Configuring WRED on Egress Queues section.

Configuring Bandwidth and Bandwidth Remaining

You can configure the bandwidth and bandwidth remaining on the egress queue to allocate a minimum percentage of the interface bandwidth to a queue.

Note When a guaranteed bandwidth is configured, the priority queue must be disabled in the same policy map.

SUMMARY STEPS

1. **configure terminal**
2. **policy-map type queuing** {[**match-first**] *policy-map-name*}

3. **class type queuing***class-name*
4. Assign a minimum rate of the interface bandwidth or assign the percentage of the bandwidth that remains:
   - Bandwidth percent:

     bandwidth {**percent** *percent*}
   - Bandwidth remaining percent:

     bandwidth remaining percent *percent*
5. (Optional) Repeat Steps 3 and 4 to assign tail drop thresholds for other queue classes.
6. exit
7. **show policy-map** [**type queuing** [*policy-map-name* | **default-8q-out-policy**]]
8. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `switch# configure terminal` `switch(config)#`	Enters global configuration mode.
Step 2	**policy-map type queuing** {[**match-first**] *policy-map-name*} **Example:** `switch(config)# policy-map type queuing shape_queues` `switch(config-pmap-que)#`	Configures the policy map of type queuing and then enters policy-map mode for the policy-map name you specify. Policy-map names can contain alphabetic, hyphen, or underscore characters, are case sensitive, and can be up to 40 characters.
Step 3	**class type queuing***class-name* **Example:** `switch(config-pmap-que)# class type queuing c-out-q1` `switch(config-pmap-c-que)#`	Configures the class map of type queuing and then enters policy-map class queuing mode. Class queuing names are listed in the previous System-Defined Type queuing Class Maps table.
Step 4	Assign a minimum rate of the interface bandwidth or assign the percentage of the bandwidth that remains: • Bandwidth percent: **bandwidth** {**percent** *percent*} • Bandwidth remaining percent: **bandwidth remaining percent** *percent* **Example:** • Bandwidth percent: `switch(config-pmap-c-que)# bandwidth percent 25` • Bandwidth remaining percent:	• Bandwidth percent: Assigns a minimum rate of the interface bandwidth to an output queue as the percentage of the underlying interface link rate. The range is from 0 to 100. The example shows how to set the bandwidth to a minimum of 25 percent of the underlying link rate. • Bandwidth remaining percent: Assigns the percentage of the bandwidth that remains to this queue. The range is from 0 to 100. The example shows how to set the bandwidth for this queue to 25 percent of the remaining bandwidth.

	Command or Action	Purpose
	`switch(config-pmap-c-que)# bandwidth remaining percent 25`	
Step 5	(Optional) Repeat Steps 3 and 4 to assign tail drop thresholds for other queue classes.	
Step 6	exit **Example:** `switch(config-cmap-que)# exit` `switch(config)#`	Exits policy-map queue mode and enters global configuration mode.
Step 7	**show policy-map** [**type queuing** [*policy-map-name* | **default-8q-out-policy**]] **Example:** `switch(config-pmap-c-que)# show policy-map type queuing shape_queues`	(Optional) Displays information about all configured policy maps, all policy maps of type queuing, a selected policy map of type queuing, or the default output queuing policy.
Step 8	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	(Optional) Saves the running configuration to the startup configuration.

Configuring Priority

If you do not specify the priority, the system-defined egress pq queues behave as normal queues. For information on the system-defined type queuing class maps, see the "Using Modular QoS CLI" section.

You can configure only one level of priority on an egress priority queue. You use the system-defined priority queue class for the type of module to which you want to apply the policy map.

For the nonpriority queues, you can configure how much of the remaining bandwidth to assign to each queue. By default, the device evenly distributes the remaining bandwidth among the nonpriority queues.

Note When a priority queue is configured, the other queues can only use the remaining bandwidth in the same policy map.

Note When configuring priority for one class map queue (SPQ), you need to configure the priority for QoS group 7. When configuring priority for more than one class map queue, you need to configure the priority on the higher numbered QoS groups. In addition, the QoS groups need to be adjacent to each other. For example, if you want to have two SPQs, you have to configure the priority on QoS group 7 and on QoS group 6.

SUMMARY STEPS

1. **configure terminal**
2. **policy-map type queuing** {[**match-first**] *policy-map-name*}

3. **class type queuing** *class-name*
4. **priority** [**level** *value*]
5. **class type queuing***class-name*
6. **bandwidth remaining percent** *percent*
7. (Optional) Repeat Steps 5 to 6 to assign the remaining bandwidth for the other nonpriority queues.
8. exit
9. **show policy-map** [**type queuing** [*policy-map-name* | **default-8q-out-policy**]]
10. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `switch# configure terminal` `switch(config)#`	Enters global configuration mode.
Step 2	**policy-map type queuing** {[**match-first**] *policy-map-name*} **Example:** `switch(config)# policy-map type queuing priority_queue1` `switch(config-pmap-que)#`	Configures the policy map of type queuing and then enters policy-map mode for the policy-map name you specify. Policy-map names can contain alphabetic, hyphen, or underscore characters, are case sensitive, and can be up to 40 characters.
Step 3	**class type queuing** *class-name* **Example:** `switch(config-pmap-que)# class type queuing c-out-q1` `switch(config-pmap-c-que)#`	Configures the class map of type queuing and then enters policy-map class queuing mode. Class queuing names are listed in the previous System-Defined Type queuing Class Maps table.
Step 4	**priority** [**level** *value*] **Example:** `switch(config-pmap-c-que)# priority`	Selects this queue as a priority queue. Only one priority level is supported.
Step 5	**class type queuing***class-name* **Example:** `switch(config-pmap-que)# class type queuing c-out-q2` `switch(config-pmap-c-que)#`	(Optional) Configures the class map of type queuing and then enters policy-map class queuing mode. Class queuing names are listed in the previous System-Defined Type queuing Class Maps table. Choose a nonpriority queue where you want to configure the remaining bandwidth. By default, the system evenly distributes the remaining bandwidth among the nonpriority queues.
Step 6	**bandwidth remaining percent** *percent* **Example:** `switch(config-pmap-c-que)# bandwidth remaining percent 25`	(Optional) Assigns the percent of the bandwidth that remains to this queue. The range is from 0 to 100.

	Command or Action	Purpose
Step 7	(Optional) Repeat Steps 5 to 6 to assign the remaining bandwidth for the other nonpriority queues.	
Step 8	exit **Example:** `switch(config-cmap-que)# exit` `switch(config)#`	Exits policy-map queue mode and enters global configuration mode.
Step 9	**show policy-map** [**type queuing** [*policy-map-name* | **default-8q-out-policy**]] **Example:** `switch(config)# show policy-map type queuing priority_queue1`	(Optional) Displays information about all configured policy maps, all policy maps of type queuing, a selected policy map of type queuing, or the default output queuing policy.
Step 10	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	(Optional) Saves the running configuration to the startup configuration.

Configuring Traffic Shaping

You can configure traffic shaping on an egress queue to impose a minimum and maximum rate on it.

Note Configuring traffic shaping for a queue is independent of priority or bandwidth in the same policy map.

SUMMARY STEPS

1. **configure terminal**
2. **policy-map type queuing** {[**match-first**] *policy-map-name*}
3. **class type queuing** *class-name*
4. **shape min** *value* {**bps** | **gbps** | **kbps** | **mbps** | **pps**} **max** *value* {**bps** | **gbps** | **kbps** | **mbps** | **pps**}
5. (Optional) Repeat Steps 3 and 4 to assign tail drop thresholds for other queue classes.
6. **show policy-map** [**type queuing** [*policy-map-name* | **default-8q-out-policy**]]
7. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `switch# configure terminal` `switch(config)#`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**policy-map type queuing** {[**match-first**] *policy-map-name*} **Example:** `switch(config)# policy-map type queuing shape_queues` `switch(config-pmap-que)#`	Configures the policy map of type queuing and then enters policy-map mode for the policy-map name you specify. Policy-map names can contain alphabetic, hyphen, or underscore characters, are case sensitive, and can be up to 40 characters.
Step 3	**class type queuing** *class-name* **Example:** `switch(config)# class type queuing c-out-q-default` `switch(config-pmap-c-que)#`	Configures the class map of type queuing and then enters policy-map class queuing mode. Class queuing names are listed in the previous System-Defined Type queuing Class Maps table.
Step 4	**shape min** *value* {**bps** | **gbps** | **kbps** | **mbps** | **pps**} **max** *value* {**bps** | **gbps** | **kbps** | **mbps** | **pps**} **Example:** `switch(config-pmap-c-que)# shape min 10 bps max 100 bps`	Assigns a minimum and maximum bit rate on an output queue. The default bit rate is in bits per second (bps). The example shows how to shape traffic to a minimum rate of 10 bits per second (bps) and a maximum rate of 100 bps.
Step 5	(Optional) Repeat Steps 3 and 4 to assign tail drop thresholds for other queue classes.	
Step 6	**show policy-map** [**type queuing** [*policy-map-name* | **default-8q-out-policy**]] **Example:** `switch(config)# show policy-map type queuing shape_queues`	(Optional) Displays information about all configured policy maps, all policy maps of type queuing, a selected policy map of type queuing, or the default output queuing policy.
Step 7	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	(Optional) Saves the running configuration to the startup configuration.

Applying a Queuing Policy on a System

You apply a queuing policy globally on a system.

SUMMARY STEPS

1. **configure terminal**
2. **system qos**
3. **service-policy type queuing output** {*policy-map-name* | **default-8q-out-policy**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `switch# configure terminal` `switch(config)#`	Enters global configuration mode.
Step 2	**system qos** **Example:** `switch (config)# system qos` `switch (config-sys-qos)#`	Enters system qos mode.
Step 3	**service-policy type queuing output** {*policy-map-name* | **default-8q-out-policy**} **Example:** `switch (config-sys-qos)# service-policy type queuing map1`	Adds the policy map to the input or output packets of system. **Note** The **output** keyword specifies that this policy map should be applied to traffic transmitted from an interface. **Note** To restore the system to the default queuing service policy, use the **no** form of this command.

Verifying the Queuing and Scheduling Configuration

Use the following commands to verify the queuing and scheduling configuration:

Command	Purpose
show class-map [**type queuing** [*class-name*]]	Displays information about all configured class maps, all class maps of type queuing, or a selected class map of type queuing.
show policy-map [**type queuing** [*policy-map-name* | **default-8q-out-policy**]]	Displays information about all configured policy maps, all policy maps of type queuing, a selected policy map of type queuing, or the default output queuing policy.
show policy-map system	Displays information about all configured policy maps on the system.

Managing Dynamic Buffer Sharing

Dynamic buffer sharing (egress buffering) within slices is configured with the global **hardware qos dynamic-buffer-sharing** command. This enables the sharing of buffers between drop and no-drop partitions. Following the command, you must save the configuration and reload the switch to enable dynamic buffering.

Example:

```
switch(config)# hardware qos dynamic-buffer-sharing
Warning: Please save config and reload the system for the configuration to take effect.
```

Note Dynamic buffer sharing requires a configured network QoS policy. For more information on configuring and applying a network QoS policy, see Configuring a User-Defined Network QoS Policy, on page 89 and Applying a Network QoS Policy on a System, on page 90.

Monitoring the QoS Packet Buffer

The Cisco Nexus 3400-S switches have a 54MB buffer that divides into a dedicated per port and dynamic shared memory. Each front-panel port has eight queues in egress. For burst or congestion situations, each egress port consumes buffers from the dynamic shared memory.

You can display the real-time and peak status of the shared buffer per port. All counters are displayed in terms of the number of cells. Each cell is 224 bytes in size. You can also display the global level buffer in terms of consumption and the available number of cells.

Note In the examples shown in this section, the port numbers are Broadcom ASIC ports.

This example shows how to clear the system buffer maximum cell usage counter:

```
switch# clear counters buffers
Max Cell Usage has been reset successfully
```

This example shows how to display the interface hardware mappings:

```
eor15# show interface hardware-mappings
Legends:
       SMod  - Source Mod. 0 is N/A
       Unit  - Unit on which port resides. N/A for port channels
       HPort - Hardware Port Number or Hardware Trunk Id:
       FPort - Fabric facing port number. 255 means N/A
       NPort - Front panel port number
       VPort - Virtual Port Number. -1 means N/A

-------------------------------------------------------------------
Name       Ifindex  Smod Unit HPort FPort NPort VPort
-------------------------------------------------------------------
Eth2/1     1a080000 4    0    13    255   0     -1
Eth2/2     1a080200 4    0    14    255   1     -1
Eth2/3     1a080400 4    0    15    255   2     -1
Eth2/4     1a080600 4    0    16    255   3     -1
Eth2/5     1a080800 4    0    17    255   4     -1
Eth2/6     1a080a00 4    0    18    255   5     -1
Eth2/7     1a080c00 4    0    19    255   6     -1
Eth2/8     1a080e00 4    0    20    255   7     -1
Eth2/9     1a081000 4    0    21    255   8     -1
Eth2/10    1a081200 4    0    22    255   9     -1
Eth2/11    1a081400 4    0    23    255   10    -1
Eth2/12    1a081600 4    0    24    255   11    -1
Eth2/13    1a081800 4    0    25    255   12    -1
```

```
Eth2/14    1a081a00 4    0    26    255   13    -1
Eth2/15    1a081c00 4    0    27    255   14    -1
Eth2/16    1a081e00 4    0    28    255   15    -1
Eth2/17    1a082000 4    0    29    255   16    -1
Eth2/18    1a082200 4    0    30    255   17    -1
Eth2/19    1a082400 4    0    31    255   18    -1
Eth2/20    1a082600 4    0    32    255   19    -1
Eth2/21    1a082800 4    0    33    255   20    -1
Eth2/22    1a082a00 4    0    34    255   21    -1
Eth2/23    1a082c00 4    0    35    255   22    -1
Eth2/24    1a082e00 4    0    36    255   23    -1
```

Configuration Examples for Queuing and Scheduling

In this section you can find examples of configuring queuing and scheduling.

Example: Configuring WRED on Egress Queues

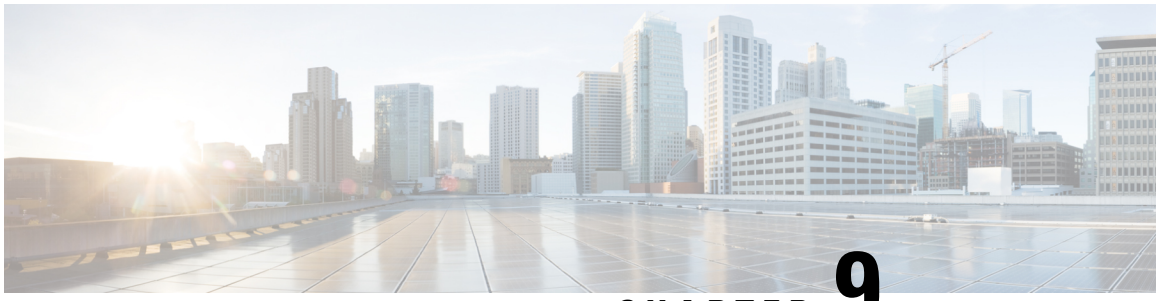
The following example shows how to configure the WRED feature on an egress queue:

```
configure terminal
  class-map type queuing match-any c-out-q1
    match qos-group 1
  class-map type queuing match-any c-out-q2
    match qos-group 1
  policy-map type queuing wred
    class type queuing c-out-q1
      random-detect minimum-threshold 10 bytes maximum-threshold 1000 bytes
    class type queuing c-out-q2
      random-detect threshold burst-optimized ecn
```

Example: Configuring Traffic Shaping

The following example shows how to configure traffic shaping using 1000 packets per second (pps)::

```
configure terminal
  class-map type queuing match-any c-out-q1
    match qos-group 1
  class-map type queuing match-any c-out-q2
    match qos-group 1
policy-map type queuing pqu
 class type queuing c-out-q1
  shape min 100 pps max 500 pps
 class type queuing c-out-q2
  shape min 200 pps max 1000 pps
show policy-map type queuing pqu
```



CHAPTER 9

Configuring Network QoS

This chapter contains the following sections:

About Network QoS

The network QoS policy defines the characteristics of QoS properties network wide. With a network QoS policy, you can configure the following:

- Pause behavior—You can decide whether a QoS group requires the lossless behavior. The lossless behavior is provided by using a priority flow control (PFC) mechanism that prevents packet loss during congestion. You can configure drop (frames with this value that can be dropped) and no drop (frames with this value that cannot be dropped). For the drop and no drop configuration, you also need to enable PFC per port. For more information about PFC, see the "Configuring Priority Flow Control" section.

Licensing Requirements for Network QoS

The following table shows the licensing requirements for this feature:

Product	License Requirement
Cisco NX-OS	The QoS feature does not a require license. Any feature not included in a license package is bundled with the NX-OS image and is provided at no extra charge to you. For a complete explanation of the Cisco NX-OS licensing scheme, see the Cisco NX-OS Licensing Guide.

Prerequisites for Network QoS

The network QoS policy has the following prerequisites:

- You must be familiar with using modular QoS CLI.
- You are logged on to the device.

Guidelines and Limitations for Network QoS

The network QoS policy has the following guidelines and limitations:

- **show** commands with the **internal** keyword are not supported.
- A network QoS policy change requires a reload.
- When enabling jumbo MTU, the default network QoS policy can support jumbo frames. Under the network QoS policy, the MTU is used only for buffer carving when no-drop classes are configured. No additional MTU adjustments are required under the network QoS policy to support jumbo MTU.
- Through the **policy-map type network-qos** command, and in the **class type network-qos** mode, the **match qos-group** number and the **pause pfc-cos** number must match.

  For example, the match and pause values (3) below are identical:

```
switch# show policy-map system type network-qos
    Type network-qos policy-maps
    ============================
    policy-map type network-qos plcy-map-1
      class type network-qos class-type-1
        match qos-group 3
        pause pfc-cos 3
        mtu 1500
```

Configuring Network QoS Policies

You can configure a network QoS policy by following one of these methods:

- Predefined policies—You can apply a predefined network QoS policy that fits your requirement. By default, default-nq-policy is configured.
- User-defined policy—You can create a network QoS policy that conforms to one of the system-defined policies.

Copying a Predefined Network QoS Policy

SUMMARY STEPS

1. **qos copy policy-map type network-qos default-nq-policy** {**prefix** *prefix* | **suffix** *suffix*}
2. **show policy-map type network-qos my_nq**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**qos copy policy-map type network-qos default-nq-policy** {**prefix** *prefix* | **suffix** *suffix*} **Example:** `switch# qos copy policy-map type network-qos default-nq-policy prefix my_nq`	Copies a predefined network QoS policy and adds a suffix or prefix to its name. A prefix or suffix name can contain alphabetic, hyphen, or underscore characters, is case sensitive, and can be up to 40 characters.
Step 2	**show policy-map type network-qos my_nq** **Example:** `switch# show policy-map type network-qos my_nq`	(Optional) Displays the type network-qos policy map.

Configuring a User-Defined Network QoS Policy

SUMMARY STEPS

1. **configure terminal**
2. **class-map type network-qos match-any** *class-name*
3. **match qos-group** *group*
4. **exit**
5. **policy-map type network-qos** *policy-map-name*
6. **class type network-qos** {*class-name* | **class-default**}
7. **pause pfc-cos** *group*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `switch# configure terminal` `switch(config)#`	Enters global configuration mode.
Step 2	**class-map type network-qos match-any** *class-name* **Example:** `switch(config)# class-map type network-qos match-any c-nq2` `switch(config-cmap-nqos)#`	Configures the class map of the type network-qos and enters class-map mode. Class network-qos names are listed in previous System-Defined Type network-qos Class Maps table.
Step 3	**match qos-group** *group* **Example:** `switch(config-cmap-nqos)# match qos-group 2`	Specifies the QoS group to match. The range is from 0 to 3. **Note** The value is this command must match the value in the **pause pfc-cos** command in step 7.
Step 4	**exit** **Example:**	Exits class-map mode and enters global configuration mode.

	Command or Action	Purpose
	`switch (config-cmap-nqos)# exit` `switch (config)#`	
Step 5	**policy-map type network-qos** *policy-map-name* **Example:** `switch(config)# policy-map type network-qos map2`	Creates a policy map. The policy-map name can contain alphabetic, hyphen, or underscore characters, is case sensitive, and can be up to 40 characters.
Step 6	**class type network-qos** {*class-name* | **class-default**} **Example:** `switch(config-pmap-nqos)# class type network-qos c1-nq2`	Refers to the class map of type network-qos as configured in Step 2.
Step 7	**pause pfc-cos** *group* **Example:** `switch(config-pmap-nqos-c)# pause pfc-cos 2`	Specifies no-drop for the QoS group. **Note** The value of this command must match the value in the **match qos-group** command in step 3.

Applying a Network QoS Policy on a System

You apply a network QoS policy globally on a system. Applying a network QoS policy also automatically applies the corresponding queuing policies.

SUMMARY STEPS

1. **configure terminal**
2. **system qos**
3. **service-policy type network-qos** {*policy-map-name* | **default-nq-policy**}

DETAILED STEPS

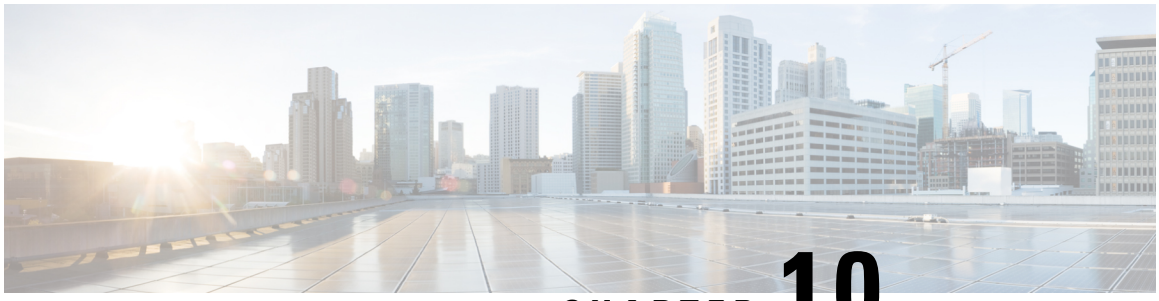
	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `switch# configure terminal` `switch(config)#`	Enters global configuration mode.
Step 2	**system qos** **Example:** `switch (config)# system qos` `switch (config-sys-qos)#`	Enters system qos mode.
Step 3	**service-policy type network-qos** {*policy-map-name* | **default-nq-policy**} **Example:** `switch (config-sys-qos)# service-policy type network-qos map1`	Specifies the policy map to use as the service policy for the system. **Note** To restore the system to the default network QoS service policy, use the **no** form of this command.

	Command or Action	Purpose
		Note All Layer 4 class-maps under the network-qos policy-map must be configured before applying it under the system qos level.

Verifying the Network QoS

To display the policing configuration information, perform one of the following tasks:

Command	Purpose
show class-map type network-qos	Displays the type network-qos class maps.
show policy-map type network-qos	Displays the type network-qos policy maps.
show policy-map system type network-qos	Displays the active type network-qos class maps.



CHAPTER 10

Configuring Priority Flow Control

This chapter contains the following sections:

About Priority Flow Control

Priority flow control (PFC; IEEE 802.1Qbb), which is also referred to as Class-based Flow Control (CBFC) or Per Priority Pause (PPP), is a mechanism that prevents frame loss that is due to congestion. PFC is similar to 802.3x Flow Control (pause frames). However, PFC functions on a per class-of-service (CoS) basis.

During congestion, PFC sends a pause frame that indicates which CoS value needs to be paused. A PFC pause frame contains a 2-octet timer value for each CoS that indicates the length of time that the traffic needs to be paused. The unit of time for the timer is specified in pause quanta. A quanta is the time that is required for transmitting 512 bits at the speed of the port. The range is from 0 to 65535. A pause frame with a pause quanta of 0 indicates a resume frame to restart the paused traffic.

Note Only certain classes of service of traffic can be flow controlled while other classes are allowed to operate normally.

PFC asks the peer to stop sending frames of a particular CoS value by sending a pause frame to a well-known multicast address. This pause frame is a one-hop frame that is not forwarded when received by the peer. When the congestion is mitigated, PFC can request the peer to restart transmitting frames.

Note RDMA over Converged Ethernet (RoCE) v1 and v2 protocols are supported on Cisco Nexus 3400-S switches.

Licensing Requirements for Priority Flow Control

The following table shows the licensing requirements for this feature:

Product	License Requirement
Cisco NX-OS	The PFC feature does not a require license. Any feature not included in a license package is bundled with the NX-OS image and is provided at no extra charge to you. For a complete explanation of the Cisco NX-OS licensing scheme, see the Cisco NX-OS Licensing Guide.

Prerequisites for Priority Flow Control

PFC has the following prerequisites:

- You must be familiar with using modular QoS CLI.
- You are logged on to the device.

Guidelines and Limitations for Priority Flow Control

Priority Flow Control (PFC) has the following guidelines and limitations:

- PFC Pause Buffer Threshold Guidelines & Limitations:
  - Ingress queuing policy allows you to optimize buffer utilization between the ports, giving certain ports a larger buffer, if needed, so long as the total buffer stays within the limit (60K * 224B). If the total buffer size exceeds the limit, the ingress queuing policy is rejected.
  - If the ingress queuing policy is accepted, the switch must be reload for it to take effect.
  - Total buffer size per block has to be managed not to exceed the limit of ~60K cells (each cell is 224B). The pause buffer limit and a large number of ports per block can cause the following limitations if the ports are configured to the default headroom
    - Long cable lengths, e.g., 300m, may cause lossless queue drops.
    - Only a single lossless class is supported (two lossless classes cannot be supported).
- Only one no-drop class is supported.
- Adding the "pause buffer size threshold" configuration is optional for cable lengths that are less than 100 meters and it does need not to be configured.

- PFC is not supported on sub-interfaces.
- For cable lengths greater than 100m, the "pause buffer size threshold" configuration is mandatory and it is required as part of the ingress queuing policy configuration, however, ingress queuing is not supported in this release.
- PFC configuration enables PFC in both the send (Tx) and receive (Rx) direction.
- Configuration time quanta of the pause frames is not supported.
- You can configure a PFC watchdog interval to detect whether packets in a no-drop queue are being drained within a specified time period. When the time period is exceeded, all outgoing packets are dropped on interfaces that match the PFC queue that is not being drained.
- The configuration does not support pausing selected streams that are mapped to a particular traffic-class queue. All flows that are mapped to the class are treated as no-drop. It blocks out scheduling for the entire queue, which pauses traffic for all the streams in the queue. To achieve lossless service for a no-drop class, we recommend that you have only the no-drop class traffic on the queue.
- You can define the upper limit of any MTU in the system using the **systemjumbomtu** command. The MTU range is from 1500 to 9216 bytes, and the default is 9216 bytes.
- For no-drop class, the supported MTU size is up to 2240 bytes.
- The interface QoS policy takes precedence over the system policy. PFC priority derivation also happens in the same order.
- Ensure that you apply the same interface-level QoS policy on all PFC-enabled interfaces for both ingress and egress.

Caution Irrespective of the PFC configuration, we recommend that you stop traffic before applying or removing a queuing policy that has strict-priority levels at the interface level or the system level.

- To achieve end-to-end lossless service over the network, we recommend that you enable PFC on each interface through which the no-drop class traffic flows (Tx/Rx).
- We recommend that you change the PFC configuration when there is no traffic. Otherwise, packets already in the Memory Management Unit (MMU) of the system may not get the expected treatment.
- We recommend WRED on a no-drop class with ECN enabled.
- ECN functions for TCP/UDP traffic. It does not function for non-IP traffic.
- Classification is supported based on DSCP/IP precedence or priority in the CoS.
- IP/MAC access-list based classification is not supported for no-drop class traffic.
- Only an exact match of the no-drop CoS is considered as a successful negotiation of PFC by the DCBXP.
- The **no lldp tlv-select dcbxp** command is enhanced so that PFC is disabled for interfaces on both sides of back-to-back switches.

Default Settings for Priority Flow Control

Table 25: Default PFC Setting

Parameter	Default
PFC	Auto

Configuring Priority Flow Control

You can configure PFC on a per-port basis to enable the no-drop behavior for the CoS as defined by the active network QoS policy. PFC can be configured in one of these modes:

- auto—Enables the no-drop CoS values to be advertised by the DCBXP and negotiated with the peer. A successful negotiation enables PFC on the no-drop CoS. Any failures because of a mismatch in the capability of peers causes the PFC not to be enabled.
- on—Enables PFC on the local port regardless of the capability of the peers.
- off—Disables PFC on the local port.

Note You can use the **priority-flow-control override-interface mode off** command to globally disable PFC on all interfaces regardless of the current interface configuration. This command, which is meant to be used during troubleshooting, allows you to quickly disable PFC without having to disable PFC on each interface.

SUMMARY STEPS

1. **configure terminal**
2. **interface** *type slot/port*
3. **priority-flow-control mode** [**auto** | **off** |**on**]
4. **show interface priority-flow-control**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `switch# configure terminal` `switch(config)#`	Enters global configuration mode.
Step 2	**interface** *type slot/port* **Example:** `switch(config)# interface ethernet 2/5` `switch(config-if)#`	Enters interface mode on the interface specified.

	Command or Action	Purpose
Step 3	**priority-flow-control mode** [**auto** | **off** |**on**] **Example:** `switch(config-if)# priority-flow-control mode on` `switch(config-if)#`	Sets PFC to the on mode.
Step 4	**show interface priority-flow-control** **Example:** `switch# show interface priority-flow-control`	(Optional) Displays the status of PFC on all interfaces.

Enabling Priority Flow Control on a Traffic Class

You can enable PFC on a particular traffic class.

SUMMARY STEPS

1. **configure terminal**
2. **class-map type qos** *class-name*
3. **match cos** *cos-value*
4. **exit**
5. **policy-map type qos** *policy-name*
6. **class type qos** *class-name*
7. **set qos-group** *qos-group-value*
8. **exit**
9. **exit**
10. **class-map type network-qos match-any** *class-name*
11. **match qos-group** *qos-group-value*
12. **exit**
13. **class-map type network-qos** *class-name*
14. **match qos-group** *qos-group-value*
15. **exit**
16. **policy-map type network-qos** *policy-name*
17. **class type network-qos** *class-name*
18. **pause pfc-cos** *value*
19. **exit**
20. **exit**
21. **system qos**
22. **service-policy type network-qos** *policy-name*
23. **exit**
24. **interface ethernet** *slot/number*
25. **priority-flow-control mode on** *slot/number*
26. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `switch# configure terminal` `switch(config)#`	Enters global configuration mode.
Step 2	**class-map type qos** *class-name* **Example:** `switch(config)# class-map type qos c1` `switch(config-cmap-qos)#`	Creates a named object that represents a class of traffic. Class-map names can contain alphabetic, hyphen, or underscore characters, are case sensitive, and can be up to 40 characters.
Step 3	**match cos** *cos-value* **Example:** `switch(config-cmap-qos)# match cos 2`	Specifies the CoS value to match for classifying packets into this class. You can configure a CoS value in the range of 0 to 7.
Step 4	**exit** **Example:** `switch(config-cmap-qos)# exit` `switch(config)#`	Exits class-map mode and enters global configuration mode.
Step 5	**policy-map type qos** *policy-name* **Example:** `switch(config)# policy-map type qos p1` `switch(config-pmap-qos)#`	Creates a named object that represents a set of policies that are to be applied to a set of traffic classes. Policy-map names can contain alphabetic, hyphen, or underscore characters, are case sensitive, and can be up to 40 characters.
Step 6	**class type qos** *class-name* **Example:** `switch(config-pmap-qos)# class type qos c1` `switch(config-pmap-c-qos)#`	Associates a class map with the policy map and enters the configuration mode for the specified system class. **Note** The associated class map must be the same type as the policy map type.
Step 7	**set qos-group** *qos-group-value* **Example:** `switch(config-pmap-c-qos)# set qos-group 2`	Configures one or more qos-group values to match on for classification of traffic into this class map. There is no default value.
Step 8	**exit** **Example:** `switch(config-pmap-c-qos)# exit` `switch(config-pmap-qos)#`	Exits the system class configuration mode and enters policy-map mode.
Step 9	**exit** **Example:** `switch(config-pmap-qos)# exit` `switch(config)#`	Exits policy-map mode and enters global configuration mode.

	Command or Action	Purpose
Step 10	**class-map type network-qos match-any** *class-name* **Example:** `switch(config)# class-map type network-qos match-any c1` `switch(config-cmap-nqos)#`	Creates a named object that represents a class of traffic. Class-map names can contain alphabetic, hyphen, or underscore characters, are case sensitive, and can be up to 40 characters.
Step 11	**match qos-group** *qos-group-value* **Example:** `switch(config-cmap-nqos)# match qos-group 3`	Configures the traffic class by matching packets based on a list of QoS group values. Values can range from 0 to 7. QoS group 0 is equivalent to class-default. **Note** The *qos-group-value* should match the **pause pfc-cos** *value*. See the **pause pfc-cos** command below in this procedure.
Step 12	**exit** **Example:** `switch(config-cmap-nqos)# exit` `switch(config)#`	Exits class-map mode and enters global configuration mode.
Step 13	**class-map type network-qos** *class-name* **Example:** `switch(config)# class-map type network-qos nw-qos3` `switch(config-cmap-nqos)#`	Creates a named object that represents a class of traffic. Class-map names can contain alphabetic, hyphen, or underscore characters, are case sensitive, and can be up to 40 characters.
Step 14	**match qos-group** *qos-group-value* **Example:** `switch(config-cmap-nqos)# match qos-group 3`	Configures the traffic class by matching packets based on a list of QoS group values. Values can range from 0 to 7. QoS group 0 is equivalent to class-default.
Step 15	**exit** **Example:** `switch(config-cmap-nqos)# exit` `switch(config)#`	Exits class-map mode and enters global configuration mode.
Step 16	**policy-map type network-qos** *policy-name* **Example:** `switch(config)# policy-map type network-qos pfc-qos` `switch(config-pmap-nqos)#`	Creates a named object that represents a set of policies that are to be applied to a set of traffic classes. Policy-map names can contain alphabetic, hyphen, or underscore characters, are case sensitive, and can be up to 40 characters.
Step 17	**class type network-qos** *class-name* **Example:** `switch(config-pmap-nqos)# class type network-qos nw-qos3` `switch(config-pmap-nqos-c)#`	Associates a class map with the policy map, and enters the configuration mode for the specified system class. **Note** The associated class map must be the same type as the policy map type.
Step 18	**pause pfc-cos** *value* **Example:**	PFC sends a pause frame that indicates which CoS value needs to be paused.

	Command or Action	Purpose
	`switch(config-pmap-nqos-c)# pause pfc-cos 3` `switch(config-pmap-nqos)#`	**Note** The **pause pfc-cos** *value* should match the *qos-group-value* in the **match qos-group** command. See Step Step 11, on page 99.
Step 19	**exit** **Example:** `switch(config-pmap-nqos-c)# exit` `switch(config-pmap-nqos)#`	Exits configuration mode and enters policy-map mode.
Step 20	**exit** **Example:** `switch(config-pmap-nqos)# exit` `switch(config)#`	Exits policy-map mode and enters global configuration mode.
Step 21	**system qos** **Example:** `switch(config)# system qos` `switch(config-sys-qos)#`	Enters system class configuration mode.
Step 22	**service-policy type network-qos** *policy-name* **Example:** `switch(config-sys-qos)# service-policy type network-qos pfc-qos`	Applies the policy map of type network-qos at the system level or to the specific interface.
Step 23	**exit** **Example:** `switch(config-sys-qos)# exit` `switch(config)#`	Exits policy-map mode and enters global configuration mode.
Step 24	**interface ethernet** *slot/number* **Example:** `switch(config)# interface ethernet 1/1` `switch(config-if)#`	Enters the ethernet interface configuration mode for the selected slot and chassis number.
Step 25	**priority-flow-control mode on** *slot/number* **Example:** `switch(config-if)# priority-flow-control mode on` `switch(config-if)#`	Enables the priority flow control policy for the interface.
Step 26	**exit** **Example:** `switch(config-if)# exit` `switch(config)#`	Exits the ethernet interface mode and enters the global configuration mode.

Configuring Pause Buffer Thresholds

To react to port congestion issues, a buffer space (pause buffer) is available to store incoming packets until the sender reacts to a system-generated pause request and stops sending packets. By default, the buffer size is automatically set by the system and is based on ingress link speed and the link cable length.

The pause buffer feature allows you to override the default buffer size by configuring buffer values in an ingress queuing policy.

Note Global ingress queuing policies are not supported.

SUMMARY STEPS

1. **configure terminal**
2. **policy-map type queuing** *name*
3. **class type queuing { queue type }**
4. **pause buffer-size** *bytes* **pause-threshold** *bytes* **resume-threshold** *bytes*
5. **exit**
6. **exit**
7. **interface ethernet** *slot* / *number*
8. **service-policy type queuing input** *name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `switch# configure terminal` `switch(config)#`	Enters the global configuration mode.
Step 2	**policy-map type queuing** *name* **Example:** `switch (config)# policy-map type queuing policy-1` `switch(config-pmap-que)#`	Enters the policy map queue configuration mode.
Step 3	**class type queuing { queue type }** **Example:** `switch (config-pmap-que)# class type queuing c-out-8q-q3` `switch(config-pmap-c-que)#`	Enters the policy map class queue configuration mode.
Step 4	**pause buffer-size** *bytes* **pause-threshold** *bytes* **resume-threshold** *bytes*	Configures the pause buffer for the policy.

	Command or Action	Purpose
	Example: `switch (config-pmap-que)# pause buffer-size 145000 pause-threshold 100000 resume-threshold 12480` `switch(config-pmap-c-que)#`	**Note** Cisco Nexus 3400-S switches do not support user-defined pause-threshold and resume-threshold as individual settings. Modification of the pause buffer size is supported using the following formula: buffer size = buffer-size - pause-threshold. For example, to set a buffer size of 32000 bytes, you can configure the pause buffer-size as 62000, the pause-threshold size as 30000, and the resume-threshold size as15000. In this configuration, the pause-threshold and resume-threshold are required, but will not be honored by the switch as individual settings.
Step 5	**exit** **Example:** `switch (config-pmap-c-que)# exit` `switch(config)#`	Enters the policy map queue configuration mode.
Step 6	**exit** **Example:** `switch (config-pmap-que)# exit` `switch(config)#`	Enters the global configuration mode.
Step 7	**interface ethernet** *slot* / *number* **Example:** `switch (config-if)# interface ethernet 1/7` `switch(config-if)#`	Enters the interface configuration mode.
Step 8	**service-policy type queuing input** *name* **Example:** `switch (config-if)# service-policy type queuing input policy1` `switch(config-if)#`	Applies the queuing policy to the interface port.

Verifying the Priority Flow Control Pause Buffer Threshold Configuration

To display the PFC pause buffer threshold configurations on all interfaces, perform the following task:

Command	Purpose
show queuing interface	Displays configuration and statistics for all ingress queuing interfaces.

Configuring a Priority Flow Control Watchdog Interval

You can configure a PFC watchdog interval to detect whether packets in a no-drop queue are being drained within a specified time period. When the time period is exceeded, all outgoing packets are dropped on interfaces that match the PFC queue that is not being drained.

Note Ingress drops are supported only on the front-panel ports.

SUMMARY STEPS

1. **configure terminal**
2. **priority-flow-control auto-restore multiplier** *value*
3. **priority-flow-control fixed-restore multiplier** *value*
4. **priority-flow-control watch-dog-interval** {**on** | **off**}
5. **priority-flow-control watch-dog interval** *value*
6. **priority-flow-control watch-dog shutdown-multiplier** *multiplier*
7. (Optional) **priority-flow-control recover interface [ethernet|ii] [intf-name] [qos-group <0-7>]**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `switch# configure terminal` `switch(config)#`	Enters global configuration mode.
Step 2	**priority-flow-control auto-restore multiplier** *value*	Configures a value for the PFC auto-restore multiplier.
Step 3	**priority-flow-control fixed-restore multiplier** *value*	Configures a value for the PFC fixed-restore multiplier.
Step 4	**priority-flow-control watch-dog-interval** {**on** | **off**} **Example:** `switch(config)# priority-flow-control watch-dog-interval on`	Globally enables or disables the PFC watchdog interval for all interfaces. This command should be configured at global and also at an interface. See the following example of the command configured at global: `switch(config)# priority-flow-control watch-dog-interval on` See the following example of the command configured at an interface: `switch(config)# interface ethernet 7/5` `switch(config-if)# priority-flow-control watch-dog-interval on`

	Command or Action	Purpose
		Note You can use this same command in interface configuration mode to enable or disable the PFC watchdog interval for a specific interface.
Step 5	**priority-flow-control watch-dog interval** *value* **Example:** `switch(config)# priority-flow-control watch-dog interval 200`	Specifies the watchdog interval value. The range is from 100 to 1000 milliseconds.
Step 6	**priority-flow-control watch-dog shutdown-multiplier** *multiplier* **Example:** `switch(config)# priority-flow-control watch-dog shutdown-multiplier 5`	Specifies when to declare the PFC queue as stuck. The range is from 1 to 10, and the default value is 1. **Note** When the PFC queue is declared as stuck, a syslog entry is created to record the conditions of the PFC queue.
Step 7	(Optional) **priority-flow-control recover interface [ethernet|ii] [intf-name] [qos-group <0-7>]** **Example:** `switch# priority-flow-control recover interface ethernet 1/1 qos-group 3`	Recovers the interface manually.

Verifying the Priority Flow Control Configuration

To display the PFC configuration, perform the following task:

Command	Purpose
show interface priority-flow-control [**module** *number*]	Displays the status of PFC on all interfaces or on specific modules.

Configuration Examples for Priority Flow Control

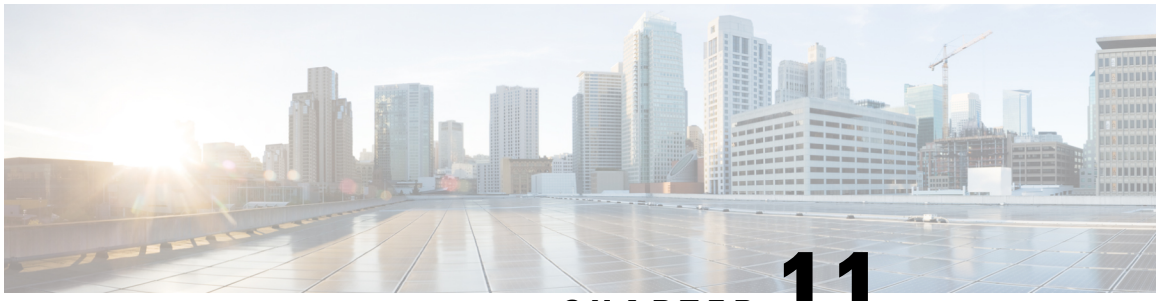
The following example shows how to configure PFC:

```
configure terminal
interface ethernet 5/5
priority-flow-control mode on
```

The following example shows how to enable PFC on a traffic class:

```
switch(config)# class-map type qos c1
switch(config-cmap-qos)# match cos 3
switch(config-cmap-qos)# exit
switch(config)# policy-map type qos p1
switch(config-pmap-qos)# class type qos c1
switch(config-pmap-c-qos)# set qos-group 3
switch(config-pmap-c-qos)# exit
switch(config-pmap-qos)# exit
```

```
switch(config)# class-map type network-qos match-any c1
switch(config-cmap-nqos)# match qos-group 3
switch(config-cmap-nqos)# exit
switch(config)# policy-map type network-qos p1
switch(config-pmap-nqos)# class type network-qos c-nq1
switch(config-pmap-nqos-c)# pause pfc-cos 3
switch(config-pmap-nqos-c)# exit
switch(config-pmap-nqos)# exit
switch(config)# system qos
switch(config-sys-qos)# service-policy type network-qos p1
```



CHAPTER 11

Monitoring QoS Statistics

This chapter contains the following sections:

About QoS Statistics

You can display various QoS statistics for the device. By default, statistics are enabled, but you can disable this feature. For more information, see the Configuration Examples For Monitoring QoS Statistics section.

Licensing Requirements for Monitoring QoS Statistics

The following table shows the licensing requirements for this feature:

Product	License Requirement
Cisco NX-OS	The QoS feature does not a require license. Any feature not included in a license package is bundled with the NX-OS image and is provided at no extra charge to you. For a complete explanation of the Cisco NX-OS licensing scheme, see the *Cisco NX-OS Licensing Guide*.

Prerequisites for Monitoring QoS Statistics

Monitoring QoS statistics has the following prerequisites:

- You must be familiar with using modular QoS CLI.
- You are logged on to the device.

Guidelines and Limitations for Monitoring QoS Statistics

Monitoring QoS statistics has the following guidelines and limitations:

- **show** commands with the **internal** keyword are not supported.
- The **show queuing interface** command can display information about internal interfaces.

  The command format for this information is specified as **ii** *x*/*y*/*z*. Where *x* is the module number, *y* is the value 1, and *z* is the internal interface number within the module.

Note The number of internal interfaces within a module varies based on the type of the line card.

Note Alternatively, you can display information about internal interfaces by providing the module number in the **show queuing** command. By including the module number, queuing information for both front-panel and internal interfaces of the module are displayed together.

Example:

```
switch# show queuing interface ii 4/1/2

slot  4
=======


Egress Queuing for ii4/1/2 [System]
------------------------------------------------------------------
QoS-Group# Bandwidth% PrioLevel                Shape
                                     Min          Max        Units
------------------------------------------------------------------
      3             -         1           -            -     -
      2             0         -           -            -     -
      1             0         -           -            -     -
      0           100         -           -            -     -
+-----------------------------------------------------------------+
|                              QOS GROUP 0                        |
+-----------------------------------------------------------------+
|                |  Unicast       | OOBFC Unicast  |  Multicast     |
+-----------------------------------------------------------------+
|        Tx Pkts |               0|               0|          235775|
|        Tx Byts |               0|               0|        22634400|
|   Dropped Pkts |               0|               0|               0|
|   Dropped Byts |               0|               0|               0|
|   Q Depth Byts |               0|               0|               0|
+-----------------------------------------------------------------+
```

```
|                              QOS GROUP 1                              |
+-----------------------------------------------------------------------+
|                |  Unicast       | OOBFC Unicast  |  Multicast      |
+-----------------------------------------------------------------------+
|        Tx Pkts |               0|               0|               0|
|        Tx Byts |               0|               0|               0|
|   Dropped Pkts |               0|               0|               0|
|   Dropped Byts |               0|               0|               0|
|   Q Depth Byts |               0|               0|               0|
+-----------------------------------------------------------------------+
|                              QOS GROUP 2                              |
+-----------------------------------------------------------------------+
|                |  Unicast       | OOBFC Unicast  |  Multicast      |
+-----------------------------------------------------------------------+
|        Tx Pkts |               0|               0|               0|
|        Tx Byts |               0|               0|               0|
|   Dropped Pkts |               0|               0|               0|
|   Dropped Byts |               0|               0|               0|
|   Q Depth Byts |               0|               0|               0|
+-----------------------------------------------------------------------+
|                              QOS GROUP 3                              |
+-----------------------------------------------------------------------+
|                |  Unicast       | OOBFC Unicast  |  Multicast      |
+-----------------------------------------------------------------------+
|        Tx Pkts |               0|               0|               0|
|        Tx Byts |               0|               0|               0|
|   Dropped Pkts |               0|               0|               0|
|   Dropped Byts |               0|               0|               0|
|   Q Depth Byts |               0|               0|               0|
+-----------------------------------------------------------------------+
|                        CONTROL QOS GROUP                              |
+-----------------------------------------------------------------------+
|                |  Unicast       | OOBFC Unicast  |  Multicast      |
+-----------------------------------------------------------------------+
|        Tx Pkts |               0|               0|               0|
|        Tx Byts |               0|               0|               0|
|   Dropped Pkts |               0|               0|               0|
|   Dropped Byts |               0|               0|               0|
|   Q Depth Byts |               0|               0|               0|
+-----------------------------------------------------------------------+
|                          SPAN QOS GROUP                               |
+-----------------------------------------------------------------------+
|                |  Unicast       | OOBFC Unicast  |  Multicast      |
+-----------------------------------------------------------------------+
|        Tx Pkts |               0|               0|               0|
|        Tx Byts |               0|               0|               0|
|   Dropped Pkts |               0|               0|               0|
|   Dropped Byts |               0|               0|               0|
|   Q Depth Byts |               0|               0|               0|
+-----------------------------------------------------------------------+
Cannot get ingress statistics for if_index: 0x4a180001 Error 0xe

Port Egress Statistics
------------------------------------------------------
WRED Drop Pkts                                  0

PFC Statistics
-------------------------------------------------------------------------------
TxPPP:                    0, RxPPP:                    0
-------------------------------------------------------------------------------
COS QOS Group        PG   TxPause   TxCount         RxPause         RxCount
   0         -         -  Inactive         0        Inactive               0
   1         -         -  Inactive         0        Inactive               0
   2         -         -  Inactive         0        Inactive               0
```

```
  3         -         -  Inactive         0         Inactive                0
  4         -         -  Inactive         0         Inactive                0
  5         -         -  Inactive         0         Inactive                0
  6         -         -  Inactive         0         Inactive                0
  7         -         -  Inactive         0         Inactive                0
--------------------------------------------------------------------------------
```

Enabling Statistics

You can enable or disable QoS statistics for all interfaces on the device. By default, QoS statistics are enabled.

SUMMARY STEPS

1. **configure terminal**
2. Enable or disable QoS statistics:
   - Enable QoS statistics:

     qos statistics
   - Disable QoS statistics:

     no qos statistics
3. **show policy-map interface**
4. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `switch# configure terminal` `switch(config)#`	Enters global configuration mode.
Step 2	Enable or disable QoS statistics: • Enable QoS statistics: **qos statistics** • Disable QoS statistics: **no qos statistics** **Example:** • Enable QoS statistics: `switch(config)# qos statistics` • Disable QoS statistics: `switch(config)# no qos statistics`	• Enable QoS statistics: Enables QoS statistics on all interfaces. • Disable QoS statistics: Disables QoS statistics on all interfaces.

	Command or Action	Purpose
Step 3	**show policy-map interface** **Example:** `switch(config)# show policy-map interface`	(Optional) Displays the statistics status and the configured policy maps on all interfaces.
Step 4	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	(Optional) Saves the running configuration to the startup configuration.

Monitoring the Statistics

You can display QoS statistics for all interfaces or a selected interface, data direction, or a QoS type.

SUMMARY STEPS

1. **show policy-map** [*policy-map-name*] [**interface** [**input** | **output**]] [**type** {**control-plane** | **network-qos** | **qos** | **queuing**}]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**show policy-map** [*policy-map-name*] [**interface** [**input**	**output**]] [**type** {**control-plane**	**network-qos**	**qos**	**queuing**}] **Example:** `switch# show policy-map interface ethernet 2/1`	Displays statistics and the configured policy maps on all interfaces, the specified interface, or on a specified data direction or QoS type.

Clearing Statistics

You can clear QoS statistics for all interfaces or a selected interface, data direction, or QoS type.

SUMMARY STEPS

1. **clear qos statistics** [**interface** [**input** | **output**] [**type** {**qos** | **queuing**}]]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**clear qos statistics** [**interface** [**input**	**output**] [**type** {**qos**	**queuing**}]] **Example:** `switch# clear qos statistics type qos`	Clears statistics and the configured policy maps on all interfaces or the specified interface or on a specified data direction or QoS type.

Configuration Examples For Monitoring QoS Statistics

The following example shows how to display the QoS statistics:

```
Global statistics status :   enabled

Ethernet6/1
          Service-policy (queuing) output:   default-out-policy

            Class-map (queuing):   c-out-q3 (match-any)
              priority level 1

            Class-map (queuing):   c-out-q2 (match-any)
              bandwidth remaining percent 0

            Class-map (queuing):   c-out-q1 (match-any)
              bandwidth remaining percent 0

            Class-map (queuing):   c-out-q-default (match-any)
              bandwidth remaining percent 100
```

The following example shows how to obtain information about queuing and PFC related counters:

```
switch(config-vlan-config)# show queuing interface ethernet 2/1

Egress Queuing for Ethernet2/1 [System]
------------------------------------------------------------------
QoS-Group# Bandwidth% PrioLevel                Shape
                                     Min          Max        Units
------------------------------------------------------------------
      3             -         1           -            -     -
      2             0         -           -            -     -
      1             0         -           -            -     -
      0           100         -           -            -     -
+-----------------------------------------------------------------+
|                              QOS GROUP 0                        |
+-----------------------------------------------------------------+
|        Tx Pkts |               0|   Dropped Pkts |               0|
+-----------------------------------------------------------------+
|                              QOS GROUP 1                        |
+-----------------------------------------------------------------+
|        Tx Pkts |               0|   Dropped Pkts |               0|
+-----------------------------------------------------------------+
|                              QOS GROUP 2                        |
+-----------------------------------------------------------------+
|        Tx Pkts |               0|   Dropped Pkts |               0|
+-----------------------------------------------------------------+
|                              QOS GROUP 3                        |
+-----------------------------------------------------------------+
|        Tx Pkts |               0|   Dropped Pkts |               0|
+-----------------------------------------------------------------+
|                      CONTROL QOS GROUP 4                        |
+-----------------------------------------------------------------+
|        Tx Pkts |              58|   Dropped Pkts |               0|
+-----------------------------------------------------------------+
|                         SPAN QOS GROUP 5                        |
+-----------------------------------------------------------------+
|        Tx Pkts |               0|   Dropped Pkts |             948|
```

+--+